Grant Agreement no. 215056

Title:	***D4.2 Platform Architecture and Design 2***
Author:	*Primary: Stephen Crane, Hewlett-Packard Laboratories Bristol, UK (HPL), with help and contributions from the WP4 team*
Editor:	*Stephen Crane, Hewlett-Packard Laboratories Bristol, UK (HPL)*
Reviewers:	*Eleni Kosta, Katholieke Universiteit Leuven - Interdisciplinary Centre for Law and ICT, Belgium (K.U. Leuven)* *Marek Kumpost, Masaryk University, Czech Republic (BRNO)*
Identifier:	*D.4.2*
Type:	*Deliverable*
Version:	*1.0*
	Date: 30.09.2010
Status:	*Final*
Class:	*Public*

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

Summary

This PICOS deliverable D4.2 Platform Architecture and Design 2 presents the second and final version of the PICOS architecture. It describes how the first architecture, which is documented in D4.1 Platform Architecture and Design 1, has evolved with lessons learnt though application and through trials based on the prototypes developed by PICOS WP5 and WP6, to create an improved/advanced technical architecture and design for the PICOS identity management platform.

As stated in PICOS deliverable D4.1, while the architecture is important, the process that has been used to define the architecture is equally significant. We began in D4.1 with real-world requirements, derived from a set of PICOS deliverables that included the views of our reference communities. This led to detailed descriptions of principles, features, system requirements and trust models, which all helped to produce a comprehensive design. We also took into account the social and legal aspects associated with operating an online member-based community of the type targeted by PICOS.

This deliverable brings together two threads of work consisting of a set of activities, an approach reflected in its two-part structure. The first part reports on the outcome of the *research thread*; the second reports on the outcome of the *prototype enhancement thread*.

One objective of this document is to integrate all of the findings of the project's first and second cycles into a single Architecture and Design document for PICOS, resulting in context-rich mobile communication services for communities that meet their participants' requirements for trust and privacy in an acceptable, trustworthy, open and scalable manner. This supports PICOS WP4's objective of providing a statement on the project's research, which can for example be used as input to the EC IST research agenda.

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
Deutsche Telekom AG	Germany
Leibniz Institute of Marine Sciences	Germany
Masaryk University	Czech Republic

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

The PICOS Deliverable Series

All documents listed below are 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
D4.1 Platform Architecture and Design v1	March 2009
D5.1 Platform description document v1	October 2009
D 5.2a Platform prototype 2a	May 2010
D6.1 Community Application Prototype 1	December 2009
D6.2a Community application prototype 2	April 2010
D7.1 a Trial Design Document	December 2009
D7.2a First Community Prototype: Lab and Field Test Report	February 2010
D7.2b First Community Prototype: Field Trial Report	August 2010
D8.1 Legal, economic and technical evaluation of the first platform and community prototype	April 2010
D9.1 Web Presence	February 2008
D9.2.1 Exploitation Planning	April 2009
D9.2.2 Exploitation Plan 2	March 2010
D9.3.1 Dissemination Planning	April 2009
D9.3.2 Dissemination Report V2	March 2010

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

The PICOS Deliverable Series

Vision and Objectives of PICOS

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

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

Planned PICOS documentation

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

PICOS results

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

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

Charter

Objectives

The objective of this PICOS deliverable is to document the technical architecture and design for the PICOS identity management platform. This includes the data model that contains the identity information, the toolbox of components that provide the identity management functions, the data flows between them and the protocols for them. The essential goals and attributes of the architecture and design are, as described in the PICOS project objectives, to cater for the identity information flow needs of new, context-rich mobile communication services for communities, whilst meeting their participants' requirements for trust and privacy in an acceptable, trustworthy, open and scalable manner.

Description of work - D4.2 Platform Architecture and Design 2

PICOS deliverable D4.2 provides both the rationale behind the PICOS architecture and a detailed description of the architecture, including high-level details of how the architecture is implemented in the platform and application prototypes.

Upon completion of the assurance deliverable (D3.1), and the evaluation report (D8.1) during the first project cycle, the architecture work was repeated during the second project cycle to create this D4.2 Platform Architecture and Design 2 deliverable. This deliverable takes account of the knowledge gained during the first cycle and of the points raised by the evaluation, in order to enrich this final version of the PICOS platform architecture.

The PICOS project's overall timescale and the activities required in each cycle means that completion of this deliverable does not coincide favourably with the prototyping work of the second cycle. This was recognised in the project's internal planning processes, and consequently it was agreed to remove the dependency of that prototyping work on this deliverable. Accordingly, this deliverable is structured around two threads: a *research thread* and a *prototype enhancement thread*.

The first thread captures the insights arising from research, which was not fully considered in D4.1, and also from the assurance and evaluation work that was undertaken on D4.1. The thread also captures new knowledge relating to architecture and design considerations that were revealed by the first cycle's prototyping and trials work. It is not mandated that this research thread should necessarily form the basis of the second cycle's prototyping work. This thread is presented in Section 2 of this document.

The second thread captures the architecture and design considerations of the second cycle prototyping work. It is included in this deliverable to document those considerations, and so forms a definition thereof that complements the detailed design documentation of the prototypes. It is a reflection on that prototyping work rather than driver for it. This thread is presented in Section 3 of this document.

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

Foreword

This deliverable D4.2 Platform Architecture and Design 2 is the collective work of the PICOS WP4 Architecture team, whose members are listed below. A substantial part of the original work in D4.1 Platform Architecture and Design 1 involved identifying and describing a wide range of components that make up the architecture. D4.2 builds on this work by considering new research and by highlighting the insights gained from actually building prototypes based on D4.1, and subsequently testing these prototypes with real-world community members.

Special mention goes to Stefan Eicker (ITO) and Widura Swittek (ITO) for contributing the approach used to describe the technical aspects of the architecture in D4.2, to the team led by Eleni Kosta (K.U.Leuven) who produced D8.1 Legal, Economic and Technical Evaluation of the First Platform Prototype, which has had such a strong influence on D4.2, to José Vivas (UMA) who provided input on assurance aspects, to Christian Kahl (GUF) for his research into advanced advertising for (mobile) communities with consideration for aspects of personal privacy, and to the team from BRNO for their contribution to standardisation and interpreting the gamer community requirements.

With thanks to the PICOS WP4 Architecture Team, and a special thanks to our reference communities and our PICOS reviewers.

The Architecture Team

Partners:

ATOS, BRNO, HPF, ITO, GUF, DTAG, UMA and HPL (all members of WP4)

and

K.U.Leuven, IfM-Geomar and Cure

Reviewers:

Eleni Kosta, Katholieke Universiteit Leuven - Interdisciplinary Centre for Law and ICT, Belgium (K.U. Leuven)

Marek Kumpost, Masaryk University, Czech Republic (BRNO)

Author/Editor:

Stephen Crane, Hewlett-Packard Laboratories Bristol, UK (HPL)

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

Table of Contents

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table of Figures

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

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

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

Table of Tables

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

List of acronyms

Abbr	*Abbreviation*
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
CA	*Certification Authority*
CS	*Client Server*
CSCF	*Call Session Control Function*
DRM	*Digital Rights Management*
DSA	*Digital Signature Algorithm*
Dx.y	*[PICOS] Deliverable: Work Package x, Deliverable y*
EC IST	*Information Society Technologies*
ENISA	*(The) European Network and Information Security Agency*
EPAL	*Enterprise Privacy Authorisation Language*
FTMGS	*Fair Traceable Multi-Group Signature*
GPS	*Global Positioning System*
GSM	*Global System for Mobile communications (originally Groupe Spécial Mobile)*
HTTP	*Hypertext Transfer Protocol*
ICT	*Information and Communication Technology*
ID	*Identity (also Identifier)*
IdM	*Identity Management (also Identity Manager)*
IM	*Instant Messaging*
IPSec	*Internet Protocol Security*
ISO	*International Organization for Standardization*
JSR	*Java Specification Request*
MAC	*Media Access Control*
OSI	*Open Systems Interconnection*
P/T/IdM	*Privacy/Trust/Identity Management*

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

P2P	*Peer-to-peer*
P3P	*Privacy for Platform Preferences*
PA	*Presence Agent*
P-CSCF	*Proxy - Call Session Control Function*
pdf	*[Trademark] Portable Document Format*
PF	*PICOS Feature*
PICOS	*Privacy and Identity for COmmunity Services*
PP	*PICOS Principle*
PUA	*Presence User Agent*
PUC	*PICOS Use Case*
RMI	*Remote Method Invocation*
RPC	*Remote Procedure Call*
RSA	*Rivest, Shamir and Adleman*
S/MIME	*Secure / Multipurpose Internet Mail Extensions*
SDK	*Software Development Kit*
S-HTTP	*Secure Hypertext Transfer Protocol*
SIP	*Session Initiation Protocol*
SLA	*Service Level Agreement*
SN/SC	*Social Network / Social Community*
SSO	*Single Sign-On*
TLS	*Transport Layer Security*
TOR	*The Onion Router*
TSA	*Time Stand Authority*
TTP	*Trusted Third Party*
URI	*Uniform Resource Identifier*
Wi-Fi	*[Trademark] Wireless local area network*
WP	*Work Package*
ZKP	*Zero Knowledge Proof*

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

Executive summary

This D4.2 Architecture and Design 2 PICOS deliverable describes an architecture for online communities, focusing on those communities with an emphasis on mobility and mobile users.

The PICOS project is distinguished in that it draws on a set of reference communities for inspiration and guidance, and in the later stages of the project for validation. The consequence of this is that the PICOS architecture is firmly grounded in the needs of today's online communities, recognising their value, the tensions and dilemmas – particularly around trust, privacy identity management and general security – that their users encounter every day.

The approach taken has been to continually cross-reference the requirements of the reference communities' with design decisions, taking care when abstracting ideas not to lose sight of the driving motivations. In fact, clearly demonstrating 'provenance' is a theme that runs through all PICOS deliverables (the extent of this cross-referencing is illustrated in Appendix H, Table 11 and 12).

The reference communities are not the only factors influencing the architecture. Legislation needs to be complied and assurance – the ability and proof that the architecture delivers on its promise – must be demonstrated. For these reasons, legal, assurance, prototyping and trialling, are key threads that run in parallel to architecture design, and have had a strong influence.

In developing the architecture, we have addressed several open questions, for example how to balance anonymity and accountability in a pragmatic and practical way. This has led to innovative solutions that the PICOS architecture captures, for example partial identities, the privacy advisor, and trust through reputation and openness. Of course, there are open research questions that to some extent remain unanswered, for example around reputation management, which we hope can be explored by future projects.

We believe that the needs of online communities are changing, with heightened awareness by users of the consequences of poor privacy and misplaced trust. Operators and developers of online community platforms and services are aware of changing attitudes, from the current open 'social networking' to controlled and considered sharing of personal information between groups of trusting individuals. The PICOS architecture is well placed to address this emerging gap in expectations between user and provider.

The 'cost' of security is often seen as an inhibitor to change, either because there is a direct financial cost that is difficult to accommodate, or because a successful business model is disrupted in some way by the changes. PICOS is conscious of this fact, and has strived to design an architecture that satisfies both requirements. Advertising is seen as a successful means to fund online communities, but the motivation of advertisers is often considered to be at odds with the privacy needs of users, especially when advertisers turn to marketing techniques directed at specific individuals.

The PICOS architecture in intended to address the needs of users, community providers and third-party organisations in a way that provides a positive benefit for all.

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

Section 1 – Introduction to D4.2

1 D4.2 Platform Architecture and Design 2

1.1 Introducing the PICOS architecture

D4.2 is a substantial deliverable, and for the most part it is organised as a reference document. Whilst this may be a helpful arrangement for the implementer and those interested in specific aspects of the architecture, it may not help readers who want to quickly gain an appreciation of what the PICOS architecture represents.

To address this concern we begin with a representation of the whole PICOS architecture that shows a high-level overview of the main elements of the PICOS architecture.

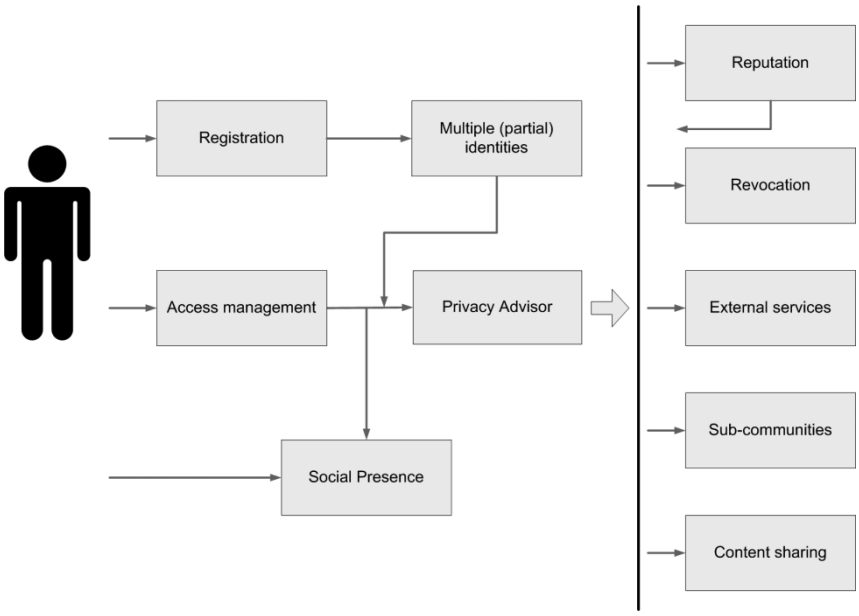


Figure 1 High-level view of PICOS architecture

Figure 1 is far from a complete representation of the PICOS architecture, but it highlights the key features, namely user management on the left-hand side and services provision on the right-hand side.

A more detailed representation is given in Figure 2, which again is not complete but which reveals in more detail some of the component grouping that provide the functionality that we later describe in detail.

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

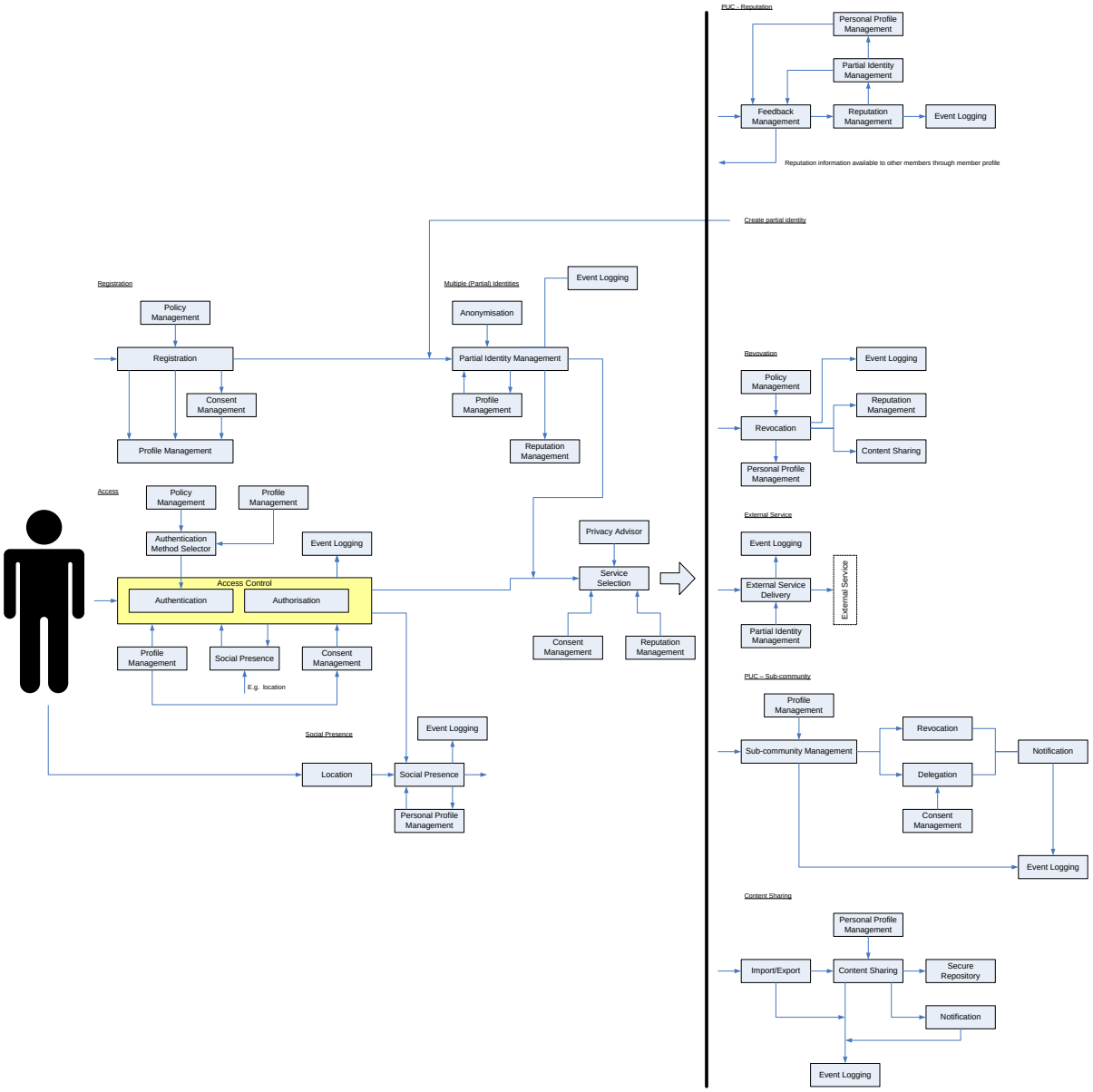


Figure 2 Detailed view of PICOS architecture

In terms of implementation, the general model is that PICOS is configured to provide enhanced functionality to existing of community services. Shown here in Figure 3, the PICOS element appears as a standalone ancillary service. In practice, the integration between PICOS and existing service is much more tightly integrated and closely coupled than this schematic suggests.

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

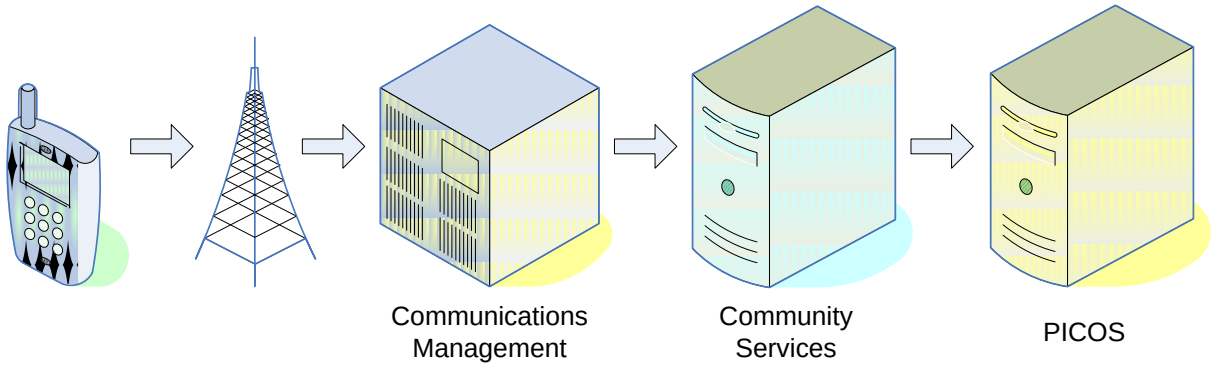


Figure 3 Implementation view of PICOS architecture

1.2 Guidance to readers of D4.2

PICOS deliverable D4.2 provides both the rationale behind the PICOS architecture and a detailed description of the architecture, including high-level details of how the architecture is implemented in the platform and application prototypes. As such, D4.2 attempts to address the needs of two audiences: 1) the Architect/Researcher, and 2) the Developer/Implementer.

D4.2 is a substantial document, which while readable 'cover to cover' is probably better treated as a reference that can be 'dipped into' as required. In order to help the casual reader navigate their way through the document, we suggest the following essential reading plan (Table 1):

Architect/Researcher	Developer/Implementer
7 Design motivations	8 Architectural views
7.1,7.2 Example scenarios	8.2.1 PICOS Components
7.6 PICOS Principles	8.3 Deployment View
7.7 PICOS Features	12.2 Building Block View
7.3 Use Case Views	13.2 ISO/IEC 29101 Example Architecture
9.3 Research outlook	Appendix E Components Descriptions
Appendix A Use Cases	
Appendix B PICOS Principles	
Appendix C PICOS Features	

Table 1 Recommended reading list

The remainder of this deliverable provides evidence to support the design decisions that we took, and offer information about the approach we took in producing the architecture. These are best treated as purely reference material.

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

In addition, in sub-section 5 we suggest a reading plan for readers interested in the less technical aspects of the architecture, namely assurance, economics and legislation.

1.3 Influences on D4.2

PICOS deliverable D4.1 was the first deliverable produced by PICOS WP4, and D4.2 is the successor to D4.1. The role of D4.2 is to provide a final architecture deliverable for the project. This deliverable takes account of earlier work, principally D4.1, and of ongoing development, trials and research that has occurred since D4.1 was produced almost eighteen months previously. D4.2 (and D4.1) draws together the work of previous deliverables, for example requirements gathering, and derives a technical description of the components that will make up a PICOS community. In so doing, D4.2 answers several important questions that define the problem that the PICOS project aims to solve, and scopes the solution in line with the aims stated in the 'Vision and Objectives' sub-section of this deliverable.

As PICOS is an EU-funded research project, an over-arching requirement, and hence influence on D4.2, is the need for the architecture to be based on and comply with the European legal framework on data protection. In the field of European Union law, the Charter of Fundamental Rights of the European Union provides for the *respect for private and family life* (Art.7) and the *protection of personal data* (Art.8), while the Data Protection Directive (1995/46/EC) has been adopted to guarantee efficient data protection. This influence has been recognised in the input from the PICOS legal research team, and taken into account in the architecture work, and is covered in sub-section 7.9, where the legal and regulatory issues relating to the PICOS Architecture are closely discussed. Deliverables D3.2 and D2.4 also had an influence on how the PICOS architectures responds to legislative requirements.

Another broad requirement of PICOS is for the architecture to accommodate an assurance analysis. This has been achieved by the active participation of the PICOS assurance researchers in the process of developing this deliverable, and is covered in sub-section 7.10.

First cycle deliverables D8.1 Legal, Economic and Technical Evaluation of the First Platform and Community Prototype, and D3.1.1 Trust and Privacy Assurance for Platform Design 1, captured the insights gained by the evaluation and assurance activities of the first cycle, and supplemented the above-mentioned participation as strong influences on the architecture work that produced this deliverable D4.2.

As previously stated, the work to create this deliverable was undertaken in two threads: a research thread and a prototype enhancement thread. Some work had a much greater influence on one thread rather than the other. Specifically, the PICOS documents that had greatest influence on D4.2 include:

- D2.3 Contextual Framework
- D2.4 Requirements
- D3.1.1 Trust and Privacy Assurance for Platform Design 1
- D4.1 Platform Architecture and Design 1
- D5.1 Platform Prototype 1
- D5.2a Platform Prototype 2
- D6.1 Community Application Prototype 1

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

- D6.2a First Community Application Prototype 2
- D7.2a First Community Prototype: Lab and Field Test Report
- D8.1 Legal, economic and technical evaluation of the first platform and community prototype

In addition, the following internal (i.e. non public deliverables) documents also influenced D4.2:

- D2.5 Community Trials Outline Plan
- D2.6 Gathering Community Requirements – Context and Role
- D5.1.d WP5 PICOS Platform Description document
- R1 Requirements for the second cycle prototypes
- R2 Investigation summary report

The following figure (Figure 4) illustrates the overall development process for D4.2

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

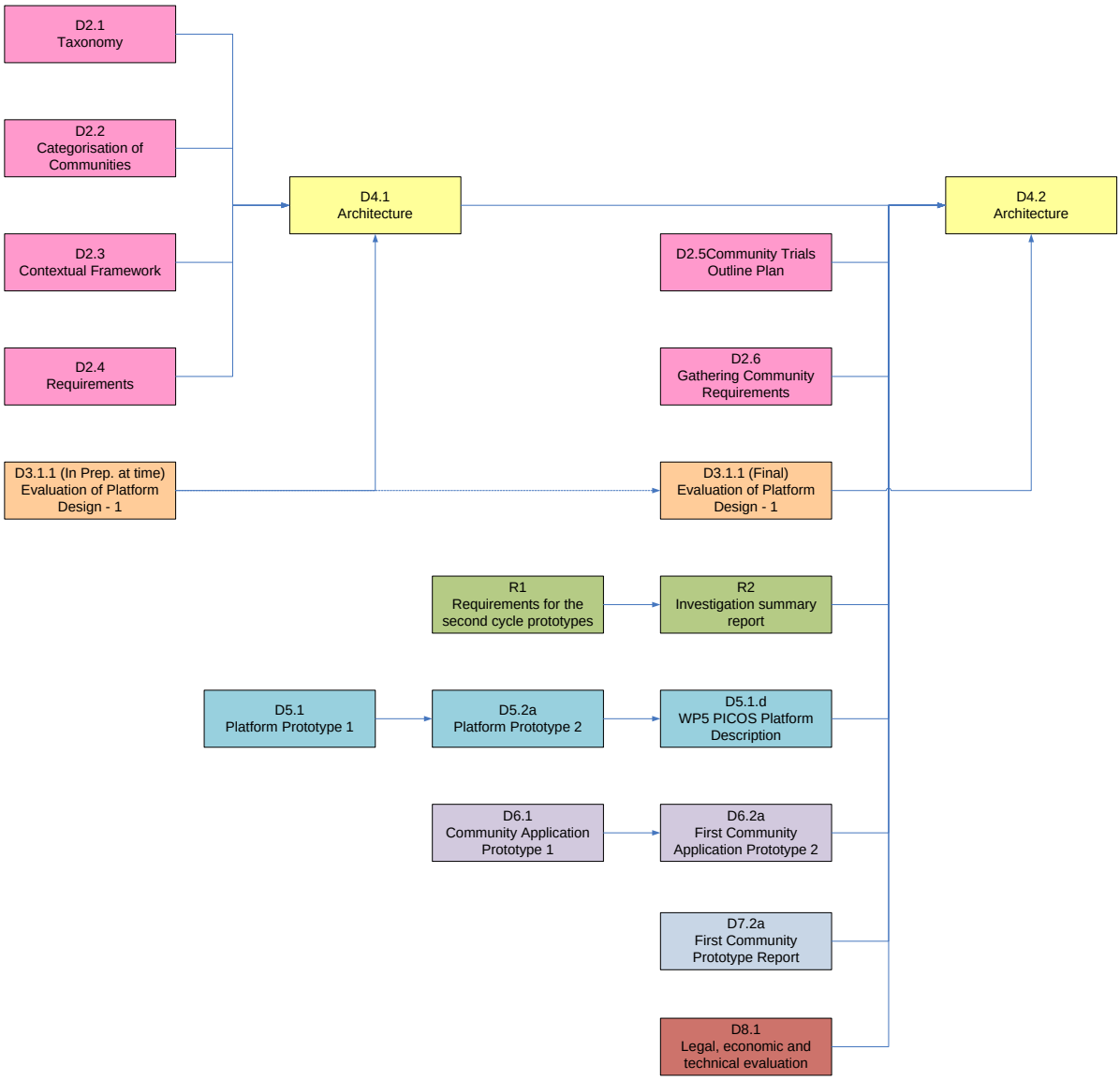


Figure 4 D4.2 development process

1.4 Architectural changes introduced by D4.2

It can reasonably be expected that in a research project, in addition to the insights gained by the creation of the first Platform Architecture and Design document (D4.1) and in its subsequent role in steering the development work undertaken by WP5 and WP6, various issues surface. To address these issues PICOS partners agreed that D4.2 would be structured around a research thread and a prototype enhancement thread, and:

- Demonstrate more clearly the connection between requirements and the documented architecture

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

- Explicitly separate the different view points to the architecture
- Review the use of tiers as a way of describing the relationship between architecture components, ensuring that the separation through levels is justified, that the role of each level is clear and that there is no overlap or ambiguity (e.g. fuzzy component naming and the interpretation of component names)
- For the parts of D4.2 that relate to the prototypes, improve the description of alignment between prototype and architecture
- Improve the structure of the document, and in particular avoid D4.2 becoming a requirements definition document
- Pay greater attention to the potential existence of multiple dependencies between components and cyclical definitions. While multiple dependencies between components is not uncommon, minimising the occurrence aids understanding. (For example, in D4.1 the Community Management defines *identity life cycle management*, which in turn depends on the Community Management component.) See Figure 5.

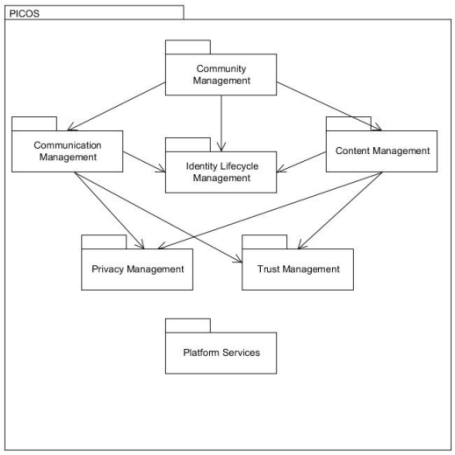


Figure 5 Example of the mutual dependency dilemma

- Address the debate about centralised control. PICOS does not implement a centralised controlling component. In fact, some features are fully decentralized or operate on a bottom-up approach. Including a central controller component with a well defined API might simplify functions like policy management and the design of the PICOS Toolbox.

To achieve some of these goals, D4.2 draws on deliverables that were produced after D4.1 was completed. It also draws on the wealth of new information that has come from the first cycle processes of building prototypes and our learning from real users, as well as from additional research.

In summary, D4.2 brings:

- An approach to meeting additional requirements
- Consideration of additional Use Cases
- A reflection of architecture-related insights gained during the first project cycle

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

- New and updated components
- Refined trust model
- New stakeholders (where requirements of third parties feature in the architecture)
- The incorporation of Assurance aspects
- The inclusion of new research
- Updated research outlook

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

2 Recap of D4.1

D4.1 started by looking at a typical scenario that a PICOS community may serve. This was an angling scenario, and was based on the experience that the project had gained from working with the angling reference community and FishBase[1]. It told a 'day-in-the-life' story of an angler, and touched on many of the privacy, trust and identity management issues that we believed PICOS is designed to address.

PICOS is interested in all communities, but especially mobile communities. We reviewed typical topologies in order to understand the physical relationship between the various entities that make up a community. Our aim was for PICOS to be as topology agnostic as was practicable.

In PICOS we focus on one very important aspect of a community, namely Trust. Every community operates under a slightly different trust model. Some communities are very trusting, while other are highly distrusting. For example, communities where members are known to one another 'off-line' are less needing of technologies that build trust. It was important to align the architecture with a trust model that best matched the type of community that PICOS is intended to address. Ideally, PICOS would support multiple trust models, and it was our aim in designing the architecture to include a wide range of models, although we recognised that in the short-term we would need to be pragmatic if the project was to meet its main goals in the limited time available.

For the outset we understood that legislation would play a critical role in defining the architecture. Compliance with privacy and law enforcement laws is mandatory, but this requirement potentially created tensions in relation to trust. It was essential that the PICOS architecture balanced these opposing demands.

We began our architecture design with a set of PICOS Principles. These were derived from past work in PICOS together with existing published research. Together these core values established the main features of the architecture.

In parallel with the PICOS Principles, we examined the main features that PICOS would deliver to users, starting with user expectations from which we subsequently derived system features.

With the Principles and key features defined, we created the architecture. First we defined and describe a broad set of low-level components, and then formed the architecture which we presented in the conclusion to D4.1.

Having designed the architecture, we tested and validated our understanding. We created a set of carefully selected use cases, which described how several of the key features of the community would be handled by the architecture. These use cases only examined a sub-set of all the possible uses that the architecture may encounter, but we believed (as has proved to be the case) that they would support the core features of the design.

In positioning D4.1, we concluded that it should describe the architecture at a high level, and should not include implementation details. However, we also recognised that in defining the architecture it would be inevitable that some implementation considerations would arise and consequently influence and enrich the design. Rather than ignore this fact, we chose to describe a practical implementation of the architecture. This description was also high-level, but contains sufficient information about

[1] Fishbase is a comprehensive database containing information about fish. http://fishbase.org

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

communications, community, trust, privacy and identity management services for the platform and applications prototypes to be created.

One of the dominant threads that ran through D4.1, and which runs through the whole PICOS project, is the belief that all decisions should be fully justified and evidenced, and that the basis for these justifications should start with our reference communities. Similarly, the earlier deliverable that produced such valuable reference information, and incidentally themselves based on investigations with our reference communities, played a key role in developing D4.1, as they do in D4.2.

Compared to D4.1, D4.2 recognises new work that influences the design of a privacy-respecting community. It describes new components and features, and presents the design in a way that is more accessible. In particular, D4.2 recognises the needs of different audiences, some less interested in the technical aspects of the design, and in so doing is more able to explain the underlying privacy, trust and identity management goal that the architecture aims to address.

In conclusion, D4.2 is an incremental advancement on D4.1, but one that provides a wealth of new information on designing PICOS-based architectures. D4.2 captures all the ideas, concepts and understanding that the project has acquired to date in one single deliverable, and can rightly be described as the definitive PICOS architecture.

In summary, D4.1 established a foundation on which to refine the PICOS architecture. D4.2 now reports on that refinement.

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

3 Building on D4.1

3.1 Why D4.2

D4.1 was the first of the two architecture deliverables that WP4 is tasked to produce. D4.1 bridged the gap between the requirements gathering exercises and the initial work undertaken by WP5 and WP6 to create the angler prototype, which turned the PICOS vision into reality.

D4.1 was necessarily focused on the immediate requirements of the target community. Nevertheless, it had sufficient scope to consider the broader issues of privacy, trust and identity management for online communities, and to subsequently embed these requirements into the architecture. In several instances, this indicated the opportunity for future research, e.g. reputation, pseudonymous identities and openness.

D4.1 positioned WP5 and WP6 to begin development of the prototype and the subsequent user trials conducted by WP7. D4.2 both refines and builds on D4.1, taking advantage of the lessons learnt in the intervening eighteen months since D4.1 was released. D4.2 extends the architecture and addresses issues raised within the PICOS team and by trial users, and essentially covers the work carried out by the project during the second cycle.

PICOS contains a research element. D4.2 provides the opportunity to report on progress made on investigating new ideas that support the PICOS architecture. This mix of research and design had led to the architecture has been created using two threads: research and prototype enhancement. Whilst supporting the architecture, the research thread is intended to look beyond the PICOS. Despite the some of these ideas not being implemented and tested, others are considered within the prototype enhancement thread and embodied in the project's second cycle prototypes. For example, privacy respecting advertising and the Privacy Advisor are carried over to the second cycle prototypes.

The split in workload between D4.1 and D4.2 is roughly 60:40, and this was reflected in the higher proportion of time devoted to implementation. In D4.2 implementation is still an important part of the deliverable, but research features strongly where concepts not implemented are discussed. Figure 6 shows how the D4.1 has evolved into D4.2.

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

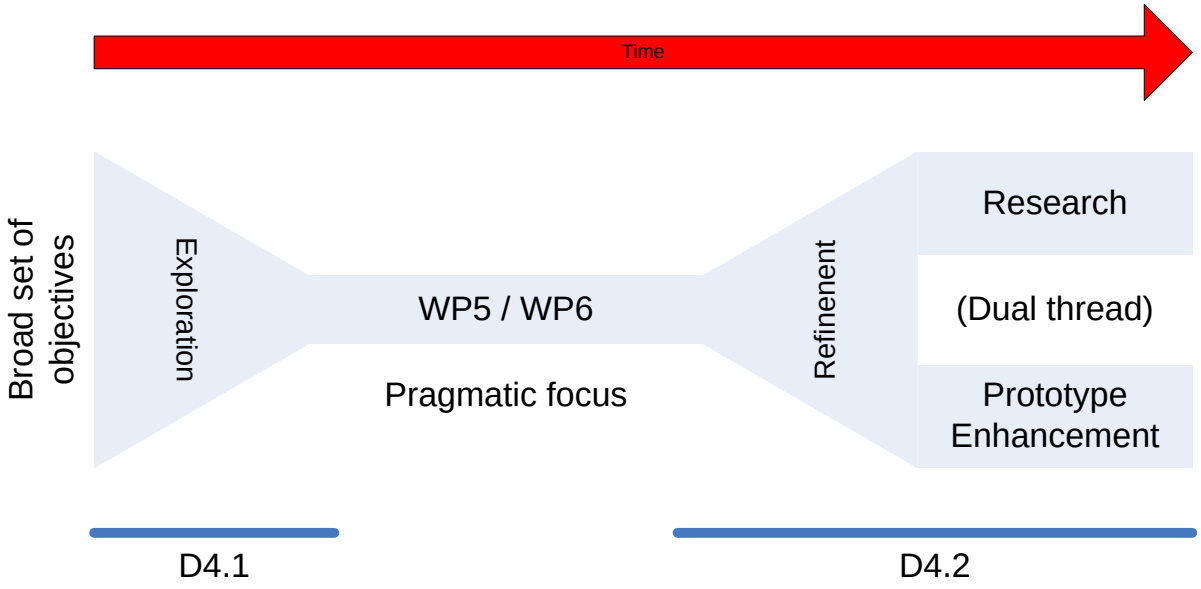


Figure 6 Relationship between D4.1 and D4.2

D4.2 is the definitive PICOS architecture, reflecting the Project's refinement of an architecture that began thirty months earlier. It is not simply a fix for D4.1; it incorporates new thinking, particularly with regard to the economic needs of a typical PICOS community – capturing funding and advertising as essential parts of community life – and clearly indicates how PICOS offers a differentiator. D4.2 reinforces the same strong emphasis on privacy, trust and identity management as core values of PICOS, which D4.1 promoted.

3.2 Drawing on the experiences of WP5 and WP6 prototypes

The first prototype was a learning opportunity for all partners, and raised many questions surrounding the provision of PICOS functionality and the practical problems that arise when trying to extend existing community platforms.

There is a strong connection between the three technical work packages, i.e. WP4, WP5 and WP6. WP5 and WP6 used the D4.1 architecture as the basis for their deliverables and, specifically, the development of prototypes. They extended the approach documented in D4.1 and gained a clearer understanding of the requirements and dependences of components and services. D4.1's features, components and the overall architecture provided a reference against which the prototypes could be built.

D4.1, through working with WP5 and WP6, established the role and importance of the Use Cases. These gave rise to a better understanding of the operation and interaction between components, implementation, and ultimately the selection of components for the first prototypes. It also helped the project decide where new technology must be created and where existing technology can be re-used.

D4.2 has also benefited from the work of WP5 and WP6, as components and concepts were built and tested, and opportunities arose to take the architecture further forward. For example, the Use Cases that were defined in D4.1, and which are so critical to a shared understanding of the architecture, have

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

been extended and improved by WP5 and WP6, for both the angler prototype and the future gamer prototype that is currently under development.

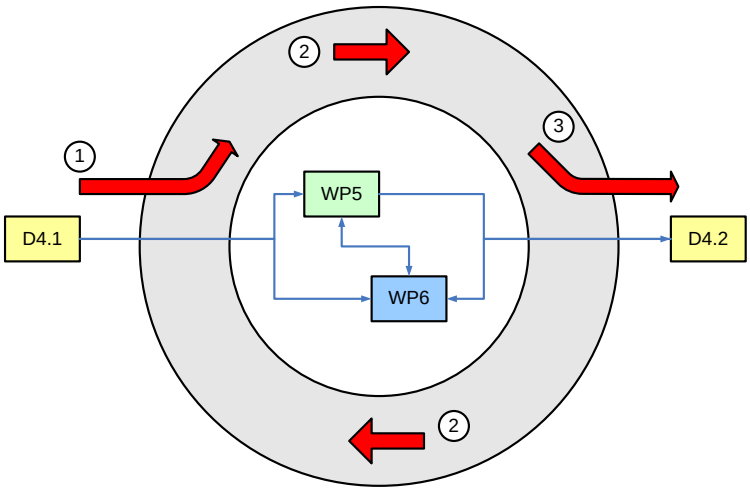


Figure 7 Link to WP5/WP6

The above Figure 7 shows how D4.1 interacted with WP5 and WP6, and what occurred post-D4.1 {1}, how the cyclic (iterative) interaction created better understanding {2}, and how D4.2 is now built on the experiences gained from all three activities {3}.

3.3 D4.2 Research thread

The research thread extends the architecture presented in D4.1 by considering a broader perspective that the project team recognised could not easily be implemented within the timescale of the PICOS project. One role of the research thread is report advanced ideas and fuel further research post-PICOS.

Although it is accepted that features identified by the research this thread will be built and form the basis of a practical demonstration, it is hoped that during the remainder of the project time will permit some of the differentiating concepts to be tested with the PICOS reference communities.

3.4 D4.2 Prototype enhancement thread

In contrast, the prototype enhancement thread tracks the development of the platform and application prototypes, capturing the changes that are being implemented 'on top of' the architecture proposed by D4.1.

The prototype enhancement thread began with a review (referred to internally as the R1/R2 reviews, and described more fully later) of requirements highlighted by the user trials. These requirements were filtered, ranked and prioritised in terms of what was valuable and feasible to incorporate into the second cycle of prototyping. The subsequent investigation phase provided a shortlist, which is described fully in Appendix F of this deliverable.

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

3.5 Changes in component naming post D4.1

In developing the architecture first presented in D4.1, several components underwent name changes. This was necessary to correctly reflect the true function of the component, taking into account minor implementation refinements. For reference, we list below these changes, organised according to the five layers of our architecture model (repeated here as a convenient reference) – Figure 8

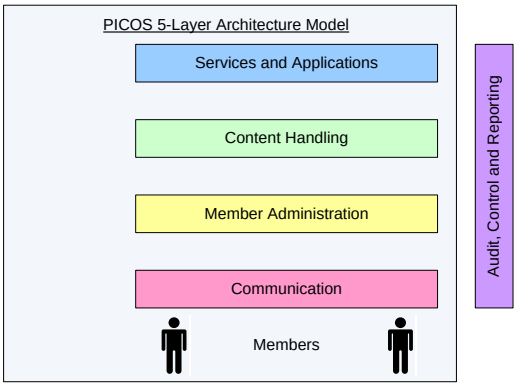


Figure 8 PICOS 5-Layer Architecture Model

Table 2 lists the original D4.1 component name and the corresponding implementation name (as recorded by WP5 in D5.1). This figure also lists the interface API that is implemented to provide the component functionality, here referred to as a service description and implemented as a WSDL (or Web Service Definition Language).

It can be seen that some components listed/highlighted are new and not defined in D4.1, and consequently have no corresponding D4.1 component.

D4.1Platform Description	D4.1 Implementation Description (D5.1)	D4.1 Service Description (WSDL)
PICOS Layer: Services and Applications		
Access Control	Proxy Web Service (part of the RPC Gateway), deployment architecture	
Anonymisation		
Application Orchestration		
Authentication	Authentication	authentication
Authorisation	Cross-cutting and Policy	
Date/Time Stamper		
External Recommendation		

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

D4.1Platform Description	D4.1 Implementation Description (D5.1)	D4.1 Service Description (WSDL)
External Service Delivery		
Feedback Management		
Identity Translator		
Importer/Exporter		
Location Sensor	Location	location
Notification	Notification component of the PRC gateway (Socket server)	notification
Partial Identity Management	Partial ID	partialid
Payment Services		
Preparation Area	Private Room	privateroomwebservice prcontentwebservice
Privacy Advisor	Privacy Advisor	privacyadvisor
Recruitment		
Reputation Management	Reputation	reputation
Scenario Management		
Service Selection		
Social Presence	Presence	presence
Trust Negotiation		
TTP Management		
Not defined at time of D4.1	Contact	contact
Not defined at time of D4.1	Centralised Database File Restoration	
PICOS Layer: Content Handling		
Content Sharing	Real-time Content Sharing	rtcontentsharing
Data Minimisation		
DRM		
Linkability		
Non-repudiation		
Secure Repository		

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

D4.1Platform Description	D4.1 Implementation Description (D5.1)	D4.1 Service Description (WSDL)
PICOS Layer: Member Administration		
Authentication Method Selection		
Consent Management		
Cryptography / Key Management		
Delegation		
Identity Lifecycle Management		
Privilege Management	Policy	policy
Profile Management	Profile	partialid
Registration	Registration Partial Identity Public Community	registration publiccommunity
Revocation	Registration	registration
Sub-community Management	Sub-community (inc. non-real-time content sharing)	subcommunitywebservice sccontentwebservice
Not defined at time of D4.1	Login	login
PICOS Layer: Communication		
Communication Management		
Network Security		
P2P Communication		
Not defined at time of D4.1	External Interface	
PICOS Layer: Audit, Control and Reporting		
Accountability		
Audit		
Event Logging	Logging	eventlogging
Event Reconstruction		

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

D4.1Platform Description	D4.1 Implementation Description (D5.1)	D4.1 Service Description (WSDL)
Intrusion Detection		
Policy Management	Policy	
Not defined at time of D4.1	Admin Console	

Table 2 Change in component naming from D4.1 to D4.2

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

4 Related EU-funded projects

There are several parallel EU-funded projects that have elements of trust and privacy as part of their vision and objectives. In developing this PICOS architecture, we have tracked and liaised with these projects to learn from and adopt approaches and technologies that complement PICOS.

The relative timing of PICOS and the other projects that we tracked have not been ideal. There were timing conflict; for example, the PEPERS project had virtually ended by the time this D4.2 architecture deliverable started. Nevertheless, it was helpful to be able to share views, discuss concepts and learn from the experiences of these others projects.

4.1 MOBIO

Project website: http://www.mobioproject.org

MOBIO is concerned with mobile services that are secured by means of biometric authentication. The project's focus on authentication provides a link with PICOS, although it is from a specific technological perspective and does not encompass the more broad /holistic approach to authentication that PICOS considers. The emphasis of PICOS is on communities in the context of privacy and trust.

Discussion with MOBIO concerned the possible integration of their already developed biometric authentication techniques. On balance it was decided that whist the biometric authentication technology had a role to play in mobile communities, the benefit of demonstrating such technology in the PICOS project had limited target appeal.

Had PICOS chosen to adopt an architecture that was less trusting of the community operator, and more client-based, stronger user authentication linked to anonymisation technologies would have been an important consideration.

4.2 PEPERS

Project website: http://www.pepers.org

PEPERS is concerned with the security of mobile peer-to-peer applications. The project has developed deep technical concepts that support general purpose platform architectures. However, the technology is not specific to social communities, and the use cases that PEPERS has developed are significantly different to those used in PICOS. Thus, there was not a strong relationship between this project and PICOS. Another factor that made collaboration with PEPERS less helpful is the fact that PEPERS was completing as PICOS started, thus it was difficult to have active exchanges with the team during the duration of our project.

Regarding P2P, this is something that was pursued with PEPERS, but ultimately we found the work unsuitable for PICOS. PICOS had adopted the approach where the community would be managed by a trusted community operator, which more closely matched the immediate needs of the reference communities and was more representative of existing community offerings, for example Facebook. It would have been difficult to include the results of PEPERS, and consequently PEPERS was not considered further in PICOS.

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

4.3 TAS3 and SWIFT

Project websites: TAS3 http://www.tas3.eu SWIFT http://www.ist-swift.eu

Both TAS3 and SWIFT were tracked, but there was not sufficient overlap in focus to benefit sharing of information.

4.4 PrimeLife and PRIMCluster

Project website: http://www.primelife.eu

(At the time of writing PRIMCluster does not have a public website.)

The PrimeLife project and PRIMCluster have both acted as reference point enabling validation of our work to be performed on a regular and on-going basis.

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

5 Structure and presentation of this D4.2 deliverable

As previously mentioned, D4.2 follows two threads: research and prototype enhancement; and to a greater extent, the presentation of D4.2 adopts a structure that emphasises this approach.

However, deliverable D8.1 taught us that there are four primary customers for this architecture deliverable. The technical development community, i.e. WP5 and WP6, which so strongly influenced D4.1 is clearly one. But there are other customers, predominantly non-technical, that have a vested interested in the architecture, and to whom this deliverable must respond.

The four key 'customers' that we have identified for D4.2 are:

- Assurance
- Economic
- Legislation
- Technical Development

We have strived to *communicate* in ways that are appropriate and effective for each customer, and ensured that the most relevant facts are presented in a concise yet comprehensible style.

A suggested reading plan for each customer is as follows (Table 3):

Assurance	Economic	Legislation	Technical Development
7.10 Assurance Perspective	7.8 Economic Perspective	7.9 Legislation	See table in sub-section 1.1
8.4 Privacy, Trust and Identity Management View	9.2.1 Advanced Targeted Advertising	13 Standardisation	

Table 3 Recommended reading list

With regard to the technical descriptions, in D4.2 we have chosen to adopt, and then adapted, an approach to describing architectures that is based on the idea of *architecture templates*. Used in the context of D4.2, templates introduce the idea of *views*, which enable an architecture to be shown from the perspective of different observers. In D4.2 we have chosen to use three views:

- Building Block View

Shows static structure of system using building blocks

- Deployment View

Shows infrastructure requirements

- Privacy/Trust/Identity Management (P/T/IdM) View

Shows most important use cases in context of its primary values

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

Figure 9 depicts the structure and presentation of this deliverable. The Appendices contain detail that applies to the research thread, the prototype enhancement thread, or both. In particular, Appendices D, E and F are relevant to the research thread, whilst Appendices A, B, C, and G are relevant to the prototype enhancement thread.

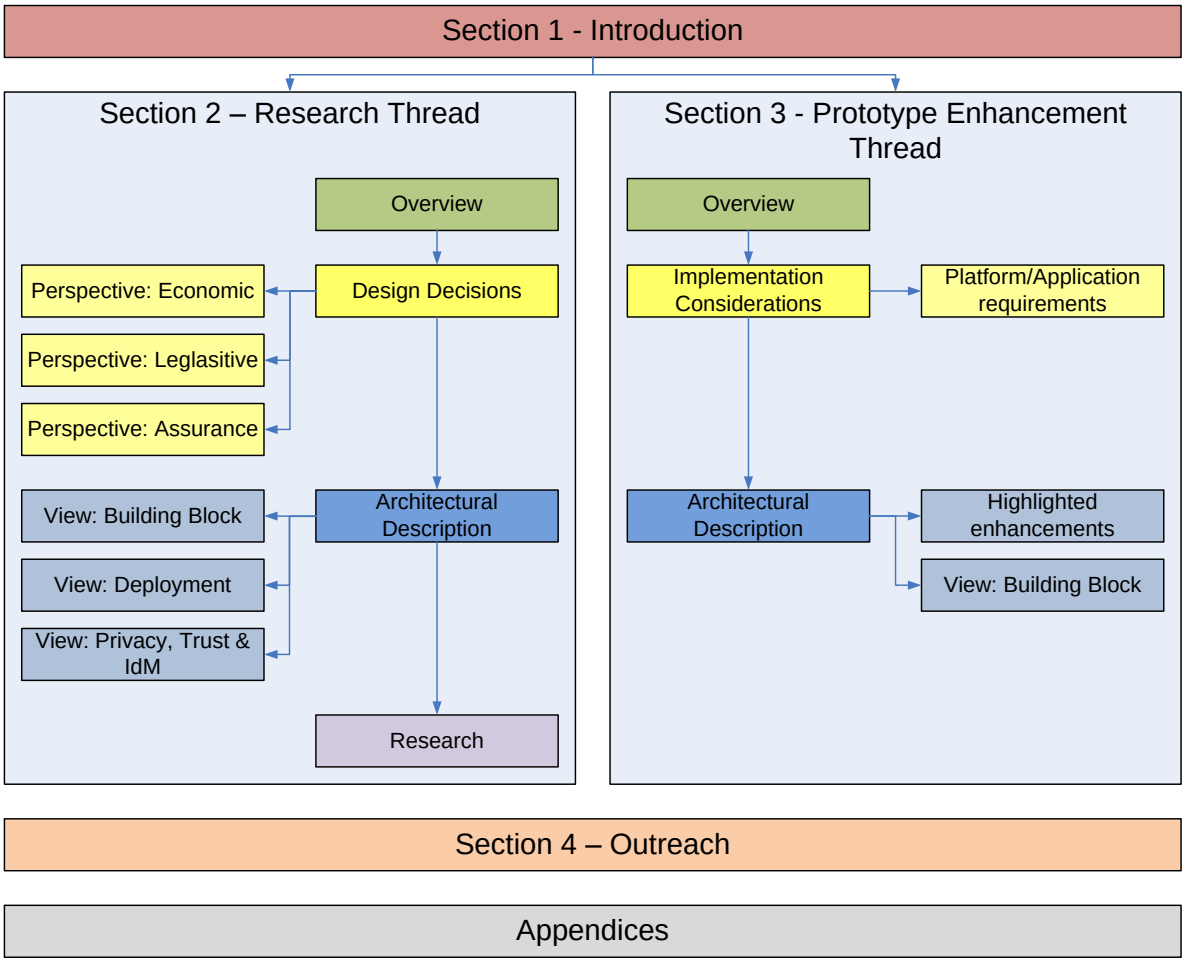


Figure 9 Structure of D4.2

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

Section 2 – Research thread

6 Overview of Research thread

The Research thread is the definitive PICOS architecture view. It takes D4.1 as a starting point, and captures the Project's design for an architecture that supports online communities. In parallel, the ongoing development of the PICOS prototypes provides an invaluable source of inspiration that has led to further innovation and research.

Areas that received attention include:

- Direct Marketing as the basis for a business model
- Privacy around member-published profiles and context-aware selective disclosure of personal information
- Implied (dynamic) member profile, such that might be used in an advertising situation to automatically profile members. This includes member observation (visibility of activities and communications) and targeted advertising based on member behaviour.
- Reputation, including reputation of (trusted) third parties.

The research thread discusses components, and relationships between the components, at a general level in keeping with the first cycle and the approach taken in D4.1.

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

7 Design motivations

In this design section we first set out two scenarios that describe days-in-the-life of two representatives of our reference community. The first scenario (7.1), which featured in D4.1, concerns John the Angler. In the second scenario (7.2), which is new to D4.2, we see Mark the Gamer engaged in some online game playing.

The two scenarios link to use cases. These have been developed specifically for PICOS to illustrate aspects of the architecture that respond to the particular situations that concern the users. For example, when joining with the community, both John and Mark use the registration component. This is described in PICOS Use Case 1{PUC1}. It is the scenarios that enable the use cases to be developed.

In addition to the scenarios and use cases, we developed a set of PICOS Principles (PP) and PICOS Features (PF). These establish aspirations for the architecture, and are based strictly on the requirements of the reference communities that were documented in earlier deliverables, e.g. D2.4. The features and use cases led directly to the components that form the architecture.

The PICOS Principles were also influenced by the needs economic, legislative and assurance needs of the project, and these in turn fed into the PICOS features too.

From the outset the project had in mind a typical community model, one that is representative of communities in existence or envisaged. It was recognised that for PICOS to have the impact intended, the architecture must observe current practices in the operation and design of community platforms, even though this could lead to compromise decisions that favour acceptance over a more purist (with regard to privacy, trust and Identity management) approach.

We refer to this 'ideal community model' as our target community, which included many of the facets of our three reference communities. From this target community emerged our trust model, which in turn directed the choice of components and features. The interaction of these design elements is depicted in Figure 10.

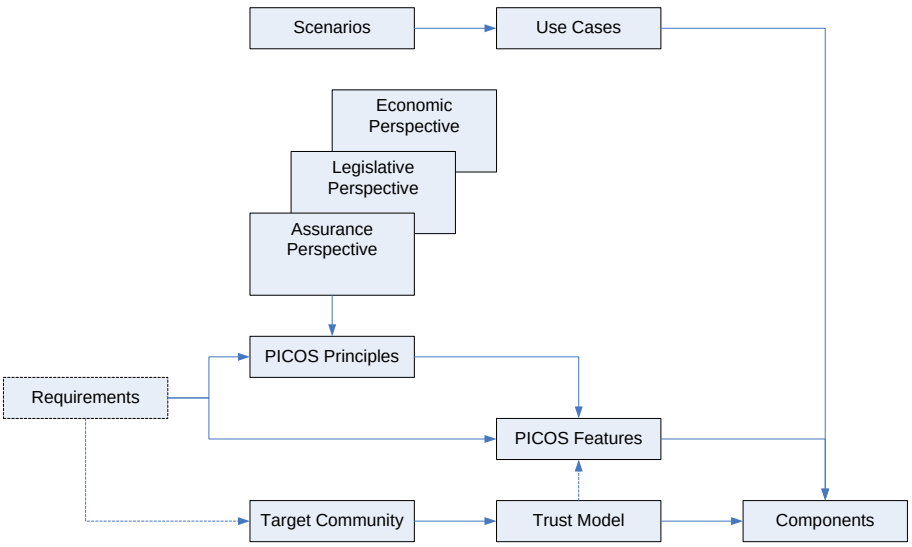


Figure 10 Design process

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

7.1 Example scenario: Anglers

In D4.1 we developed a user scenario to help us understand how users might interact with a PICOS community, and indeed what they might want from such a community. The scenario was artificial – an imaginary user experience – which tells the story of a typical day-in-the-life of someone who we anticipated would benefit from using a PICOS enabled community.

Studying the angling community helped us gain a good understanding of what PICOS should deliver, and allowed us to scope the project. As far as possible the first iteration of the architecture attempted to capture and address the tensions that this scenario predicted. At that stage no decisions had been taken to implement any features that arose from the scenario, and it was accepted that what was eventually implemented might conceivably have nothing to do with this scenario at all.

Our scenario was based around John. We attempted to show how the features that John desired could be realised by the PICOS community. We did this by inserting references to PICOS Use Cases (PUCs) that we had developed separately (and are described in Appendix A, where a reference {PUCn} refers to Use Case n.

The angler story as told in D4.1 is repeated below. For D4.2 we have also developed a gamer story, which also follows.

7.1.1 John, the Angler: An angling holiday

John is an experienced angler, especially in catching fish that live in the North Sea and adjacent waters, such as the North Atlantic and the Baltic Sea. On the occasion of his 40th birthday, his fishing buddies decided that John should try fly-fishing, so they gave him a basic fly-fishing set as a birthday gift. However, John has never attempted fly-fishing before, but believes that this fishing method is really worthwhile trying. In order to get a comprehensive idea of what fly fishing could be like, he decides to spend his next vacations in the mountains of Bavaria, where he can expect a number of promising sites for fly fishing. In preparation of his vacation, he found a fly fishing simulator on the Internet, which he considered useful for getting an idea for what fly fishing is like. Playing with the simulator gave him an idea; Fly-fishing could be a lot of fun, but it is also a fishing technique which needs a lot of skill and knowledge about the ecology of the target fish and their environment.

7.1.2 John's concerns about technology

John is not a technology expert, but he is reasonably comfortable using the Internet; he sends emails and checks his bank balance online regularly. He is aware that the Internet presents a risk, but beyond knowing not to respond to Spam emails with his bank account details, and to watch out for viruses, he isn't sure what he needs to worry about or how to protect himself. He knows that people steal personal information and that hardly a day seems to go by without there being a report in his newspaper saying that another government department or company has lost personal data.

Besides the membership in a regular fishing club, 'ASV Nordseekant' which is located in the city where John lives, he is a member of an online marine angler's community. He noted that a group of anglers in this community indicated a while ago that they have experience in fly fishing. So John logs in to his angling community and is asked to register with the group. On this occasion John is accessing the website from his home PC, but since the community also supports access from mobile devices he expects to use his mobile phone to gain access once he leaves on his trip.

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

7.1.3 John registers with a community

John provides the requested personal information, including an angling credential that states that he is entitled to fish at his chosen location {PUC1}. John's angling community provides a service which allows members to sign in and apply online for a rod license for marine fishing, which is issued by the governmental fishing authority. This is a credential which is endorsed, and which provides evidence of John's right to fish in the said waters {PUC1}. The information provided is authenticated, and John is subsequently granted access to the thematic groups in his community about fly-fishing and he was searching for information he needs to plan his fly-fishing trip {PUC2}.

7.1.4 John joins a group

When John registered, he created a profile that defined what information about John other members can see {PUC1}. He can also create a group – a buddy list – where he can list the other anglers he will interact with on a regular basis {PUC9}. John decided to join the existing discussion group on fly fishing. However, since he was afraid, that he can be blamed because of its little knowledge, he wanted to discuss fly fishing issues also only with known buddies and he decided to create his own group on this topic {PUC9}. Initially, he invited just his known friends to become members of this private room, but he was already considering opening this group to all other community members when he would be a bit more experienced. This is all handled by the social relations facility, which is responsible for managing and graphing John's connections to other community members {PUC7}.

7.1.5 John sets his privacy preferences

The profile also permits John to set privacy preference settings which, among other things, allow John to automatically disclose his social presence management component which shows John's online presence, an indication of his online status and location. His buddies or other anglers can check if John is online and available to chat, just as John can check the status of other users {PUC8}.

7.1.6 John searches for recommendations

Before John starts his fly-fishing vacations he would like to get recommendations for promising angling spots and other necessary infrastructure such as restaurants, tackle shops and licensing rules and regulations around the anglers hotel he has booked for his vacations. John considered becoming a temporary member of one of the local Bavarian online angling communities which was recommended from his friends in his marine angler's community {PUC4}.

7.1.7 John logs in

With his angling vacations approaching, John frequently logged in into the Bavarian online angling community and tried to find the respective information posted from other members of the community. As a registered member, John can upload photographs and download angling information, and communicate with other users {PUC7}. When logging in, John will need to prove his identity, by using his chosen authentication mechanism from the set of mechanisms that the angling community supports {PUC2}. John did not need to register again for temporary membership in the Bavarian online community on fly-fishing, since with his membership in the marine anglers community, he is automatically and transparently granted access to all other angling-related communities and web sites

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

that he wants to visit when preparing the fishing trip. The facility, known as federated access, also allows John to use online services for which he has not registered. This is because through mutual agreement, John's registration credentials are accepted by other service providers.

This is especially useful, since some of this information that John needs is provided by third parties, for example weather information or qualified biological information from FishBase about the local fish fauna including identification tools and field guides he can print or he can use from his mobile device {PUC6}. If John ever decides to fish in another area it means he does not have to register with a new community every time. John simply takes advantage of a federated access service that allows him to automatically gain access to the new community.

7.1.8 John checks reputation

While searching for local information, John also wants to see user-generated recommendations for the results of the search. A recommendation is only useful if he can get additional information on the person who made the recommendation, e.g. their profile, their reputation in different communities and their relationship to John {PUC5}. This is only possible because the community offers an identity management component allowing the federation of partial identities, and thus cross-community reputation and recommendation.

7.1.9 John configures location and privacy settings

John suspects that at this time of the day two fishing family members and another Swiss friend, Jean-Paul, may also be logged in to his main online community. He checks his buddy list for their status and location {PUC8}. Of course, this is only possible if John's family and friends have granted John right to see this information, which they will have configured using their own social relations facility.

John can see his family members, but his friend, Jean-Paul, is currently blocking access to this information because he probably has privacy concerns. So, John decides to communicate directly with Jean-Paul using the community's instant messaging service. John writes to ('texts') Jean-Paul, who fortunately is logged in. He is alerted by his vibrating Smartphone and reads the message from John asking for access to Jean-Paul's status (presence) information. Attached to John's message, Jean-Paul receives a digitally signed statement issued by the Reputation Management component, which convinces Jean-Paul that he can trust John {PUC5}. In response, Jean-Paul also grants John access to his social presence information, simply by updating his privacy preferences {PUC8}.

As John and Jean-Paul are holidaying together in the Alps later in the year and want to go fishing together, Jean-Paul also grants John access to his location information, but only during the days he knows they will be in the same holiday area. This is again managed by the privacy preferences and social presence facility.

John immediately sees the new information and has a great idea. He sets up a group using the Group Management facility so that he and Jean-Paul can share specific information to help with planning the trip; e.g. he would be able to deliver his exciting experience to this group straight from the watercourse, using his Smartphone {PUC9}. Although personal information will be shared, both friends are confident because they know that no one outside the Group will have access {PUC7}. They also realise that during and after the planned trip they can share photos and other (multi-media) information showing the great catches that they expect to make.

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

7.1.10 John accesses another community

Finally having arrived in the angler's hotel, John decides to join another angling community, which is suggested from a member of the Bavarian online angling community as a group of fly fishing specialists who knows the fishing sites where John wants to go fishing in his vacation very well. Normally this community is restricted to register members because they want to hide their special knowledge within a limited number of members. Only users of good repute can access the community. Because John has not been member before, his reputation is unknown {PUC5}. Fortunately, John has been a good member of another community and he can transfer that reputation to this new community as proof that he can be trusted.

7.1.11 Authentication

The new angling community needs to verify John's identity and that John is indeed the member of the other angling communities. This is possible because of a federated identity management system which provides community membership management and trust management across communities. (Of course, if the local community does not know the other communities then the local community must decide dynamically how much to trust John). Once John's identity has been validated and he has been granted temporary access to the members-only area of the community site, other members of that community can see John's profile, and can see the reputation that he has established in the other communities before and has chosen to disclose.

Upon arrival at the water course, John realised that he has forgotten a number of items necessary for a successful fishing day, such as flies which are due at this time of the year. Thus he searches for a local tackle shop on his Smartphone, and he sees recommendations that have been made by members of the local angling community {PUC5}. Those will be presented as recommendations coming from fellow members of the community that he now belongs to. John can also see if any of those members are currently online, and if so he has the possibility of communicating with them directly, i.e. he can ask for advice in real-time. Any community member can control who can see their status. Members can also control who can contact them directly. For example, some members may prefer to only accept messages from registered members, as opposed to guests.

7.1.12 John posts feedback

Having visited the tackle shop and gathered the needed equipment based on excellent advisements of the tackle shop owner, John decides to share (post) his own recommendation about the shop on the shop’s website. Rather than posting as an anonymous user, he decides to post it using his local angling community identity. The shop website verifies that John is indeed that member of the local angling community.

This recommendation encourages John to purchase items using his mobile device from the online shop. This is very convenient for John, since the shop delivers the chosen items to John’s hotel. However, the shop needs John to first supply some sensitive personal data.

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

7.1.13 John wants to be anonymous

John is excited about finally going fishing, but in the back of his mind there are those concerns about security and privacy. He wonders why he should trust the community to look after his information. Has he made a terrible mistake that he will live to regret? But then he remembers he also joined the local community because he wanted to get to know more local anglers who can help him to make the fishing trip successful, so perhaps he needs to be more relaxed about all this privacy stuff. After all, it's probably all hype to get people to buy credit card insurance! He decided then to share photographs of the fish he catches, the location, the date and time caught, and his experience with successful baits. However, he thinks that he doesn't mind telling his new angling friends from the local online community, who he already knows well, but he doesn't want the whole world to know about his special experience.

7.1.14 John makes a payment

Still a little concerned, John decides to investigate further, and discovers something called anonymisation and pseudonymisation, which apparently means that John can interact with others without telling them his real name. Sounds like the ideal solution. When John makes a payment or provides evidence of entitlement, non-essential personal information is obscured.

John also discovers that he can restrict who can see his information through something called access control {PUC7}. This is really easy to do since he only needs to set a few options in his personal profile and that's it.

7.1.15 John terminates his membership of the community

At the end of the fly fishing vacations, John can choose to cancel his membership in the special local online community, or he can wait for it to expire automatically {PUC3}. However, even though he has left the community, the history of his membership, messages that he posted, and any reputation that he established, is maintained by the local angling community. Before leaving the community John decided to post photographs of his trip including the fish he caught. As an acknowledgement of their useful tips and trips which promoted John's success as a fly fisher, other members can still see the photos of the catch, even though John is no longer a member of the community. Since he behaved according to the rules of that community and since he provided content, he was rated from community members as a trusted fishing buddy and his reputation score (which never expires and can be transferred to other communities) was increasing which may facilitate to access special groups in other online angling communities in the future {PUC5}.

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

7.2 Example scenario: Gamers

7.2.1 Mark, the Gamer: One epoch in a game

Mark is an experienced online gamer. He has just decided to play a new epoch (or round) of his favourite game. An epoch of one game ends if any alliance manages to build the *world wonder*. The duration of one epoch is typically in order of months.

Mark has a solid experience of this game because he already played several epochs. In two epochs he was a member of a winning alliance. That gave him a lot of experience, increased his reputation and also brought new friends among the gamers. But once the epoch was over almost all connections with these people were lost and he never met them again. He stayed in contact with only some of his best friends/players, and at the beginning of a new epoch they decided to cooperate by creating an alliance. The meant that Mark could begin the new epoch with experience that he had developed from previous epochs and friends with which he had cooperated. Mark therefore knows what he can expect from his 'team' when times are hard for the alliance.

7.2.2 Mark's concerns about technology

Mark has a solid experience of technology. He actively uses social networks and he uses mobile device and computer daily. Mark is also aware that such technologies present certain risks, both security and privacy, and he has developed some knowledge about possible means of protection. He knows of the risk from people who spy/steal/misuse personal information, since hardly a day seems to go by without there being a report in his newspaper saying of the loss of personal data and the resulting consequences for the individual affected.

Mark is a member of an online gaming community, which he accessed while playing his last online game. He noted that a group of gamers in this community considered Mark to be a responsible and cooperative player. This reputation helped Mark gradually become a player who creates strategies and advises other players how they should play. Mark would very much like to retain his newly acquired reputation as starts playing new online games, or even transfer it to other communities.

Mark accesses the game via a website using his home PC, but since the community also supports access from mobile devices, he sometimes uses his mobile phone to gain access and talk to his friends.

7.2.3 Mark registers with a community

Mark provides the requested personal information to the community, including his past game/playing experience. The information provided is authenticated, and Mark is subsequently granted access to the community discussion board. This discussion board is often the only place where Mark can meet with other players (some of them are already known to him from previous games/epochs) from his community in order to discuss game strategies, plan alliances, etc.

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

7.2.4 Mark sets his privacy preferences

Mark's profile, which is held in the discussion board, permits Mark to set privacy preference settings that, among other things (e.g. email address, real name, age, postal address, ...), control the automatic disclosure of his online presence, i.e. provides an indication of his online status to other members. Thus, Mark's buddies (or any other gamer) can check if Mark is online and available to chat. Similarly, Mark can check the status of other members too {PUC8}.

Mark can also specify his contact email address(es) or postal address as well as his telephone number(s). Since he wants to use only the built-in messaging system (sometimes called "private message"), he does not fill-in any of this information in his profile. (He thinks he probably would do so if he could control access and check who viewed information contained in his member profile, and what type of information was viewed.) Since the discussion board requires this information in order to complete the registration process, Mark simply fills-in some fake information.

7.2.5 Mark logs into the discussion board

As a registered member, Mark can upload photographs, download available information, and communicate with other users {PUC7}. When logging in, Mark will need to prove his identity, which he does using his chosen authentication mechanism from the set of mechanisms that the discussion board supports {PUC2}. There are several roles in the discussion board (moderator, power user, ordinary user) that Mark can perform, but this option typically depends on his reputation and online activity.

7.2.6 Mark checks reputation

When searching / retrieving information about players (e.g. location, 'closeness' their historical activities/abilities while under attack), Mark wants to receive user-generated recommendations to support the results of a search. Retrieved information is only really useful if Mark can obtain additional information about the person who provided the information, e.g. the other member's profile, their reputation in different communities and their relationship to Mark {PUC5}. The problem for Mark is that it is usually not possible to directly transfer reputation scores from other (past) discussion boards (from previous epochs) since they are not normally compatible with the new installation that is used at the beginning of a new epoch.

7.2.7 Mark accesses another community

As Mark plays the game he reaches a point where he realizes that it will be good for him to change his alliance membership. This is because his current alliance is not very cooperative and active, and its members are facing several attacks without a solid defence. He tries to contact the leaders of stronger alliances in order to discuss options for becoming a member of their alliance.

Mark finally receives an offer from a very strong alliance that is willing to accept him as a new member. This is very good news for Mark because it is not very often that a strong and cooperative alliance accepts new (typically unknown) members. As Mark is joining as a new member, he has to register (and obtain access) to a new discussion board. Leaders of his old alliance will also receive the information that Mark has changed his alliance, and will take all steps possible to prevent Mark from

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

accessing the old discussion board. The main reason is that this dual-membership can be exploited by another alliance.

7.2.8 Mark wants to be anonymous

Mark is excited about becoming a member of such a strong alliance, but at the back of his mind he still has concerns about security and privacy. He wonders why he should trust the community to protect his information. Has he made a terrible mistake that he will live to regret? But then he remembers he joined the community because he wanted to be a member of a strong alliance and to win the game, so he becomes more relaxed about 'all this privacy stuff'. He then decides to share photographs and screenshots taken from the game and a recent 'gaming' party. However, he knows that this content would remain within the community long after he has left (e.g. if something bad happens and he is kicked out). So he decides not to disclose any content that he feels is personal and privacy-sensitive, e.g. his car with an identifiable number plate number.

7.2.9 Mark offers to share his gaming tools

Since Mark is an experienced gamer, over time he has created his own "beyond-the-game" tools that help him to better analyze his battles (e.g. battle simulator, distance and time calculator, soldiers power calculator). He is willing to share this set of tools with members of his alliance, but he doesn't want the tools to be publicly available. He knows that he cannot control the spread of his tools within his community – a member of his alliance may disregard his request no to share them – but he decides to offer them to others during the latter stages of the game, which is when he has greater knowledge of his colleagues in terms of their reputation. He is surprised that he receives very positive and warm feedback about his set of tools.

7.2.10 Mark organizes a meeting in a pub

As the game is almost at its end Mark and other leaders of his alliance decide to organize a face-to-face meeting in order to meet personally with other players. They know each other quite well in the online world but never met each other in the real world. Other members are willing to provide Mark with their mobile telephone numbers in order to be easily reachable.

Mark chooses his favourite pub and sets a time for the meeting. Almost half of the whole alliance joined Mark, and had a very nice time together. As a result, Mark met new people and discovered that some had some similar interests to his own (besides online gaming), and Mark made several really good new friends.

7.2.11 Mark terminates his membership of the community

At the end of game epoch Mark can cancel his membership of the discussion board used by his alliance. But it is normal practice for discussion boards to be deleted after the game ends, and those who want to stay in contact have to exchange their contact information before the end of the game epoch. Mark met some interesting people that he wants to stay in contact with, so he puts those people into his local contact list (e.g. into his mobile phone contact list). This contact list cannot be shared and is not online.

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

7.3 Use Case views

To illustrate how the architecture solves practical day-to-day situations which our target community may encounter, and to indicate the interaction between components, we identified 15 PICOS Use Cases (PUC) in D4.1. Use cases are used to show the most common interactions.

Each use case has been selected because it satisfies an element of the scenarios previously described, and because from experience we know that the trust and privacy issues that PICOS will raise require a detailed level of understanding of user interactions.

Of these 15 PUCs, in D4.1 we explored the first nine to better understand the interaction between components. These nine were considered higher priority PUCs because they cover the application of the core privacy and trust management components.

Later, WP5 introduced a new use case (referred in D5.1 as PUC 10) to explain how privileges are managed. This is now included in this D4.2 as PUC 16, and described more fully in Appendix A.

Further use cases (or refinements to existing use cases) arose from the trials, and these are also included and referenced as PUCs 17-23. They relate only to the online gaming community.

(Note that the order of this list does not imply any priority.)

- **PUC 1: Registration**: Registration and creation of a new member profile. Creating an initial identity, importing reputation, setting policies and respecting different roles. (Note: The gamer community needs an enhanced set of attributes that extends the list specified by the anglers.)
- **PUC 2: Accessing the community**: Identifying, authenticating and granting authorisation to a member. Selecting a service.
- **PUC 3: Revocation**: Leaving a community, giving due consideration to content contributed by a member.
- **PUC 4: Multiple partial identities**: Creating, selecting and managing multiple member identities (pseudonymous/partial identities).
- **PUC 5: Reputation**: Establishing the reputation of members within and across communities. Providing recommendation and feedback. Registering to receive notifications. (Note: In the gamer community, reputation is extended to the 'points of interest'.)
- **PUC 6: External services**: Exposing partial identity / profile to external services
- **PUC 7: Content sharing**: Importing/exporting and controlling the sharing of content contributed to the community by members, including automatic/manual tagging and notification. (Note: In the gamer community, access is linked to content and date.)
- **PUC 8: Presence**: Setting and controlling the sharing of online status information (location, presence, etc.) about members.
- **PUC 9: Sub-community**: Creating and managing a sub-community (sub-group) within the overall community.

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

D4.1 also noted six additional use cases (PUC10-15) that we expected to prove useful. However, in practice that proved less useful, and was subsequently superseded by seven new use cases (PUC16-23). These six new use cases are listed below and described in Appendix A.

- **PUC 10: Community reputation**: Check and validate the reputation of a community (prior to becoming a member). Establishing, and making publicly available, the reputation of a community, for the use by new members considering joining the community.
- **PUC 11: Searching**: Searching for and establishing contact with other members within the community, who share similar interests.
- **PUC 12: Offline working**: Enabling member to benefit from community services when offline (typically mobile)
- **PUC 13: Feedback**: Providing recommendations / feedback. See also PUC 19 for a link between reputation and advertising.
- **PUC 14: Real-time communication**: Allowing member to interact one-to-one, thus sharing content in real-time.
- **PUC 15: Audit**: Audit, correcting errors, removing privacy-violating content

The following eight use cases are new to D4.2:

- **PUC 16: Privileges**: Controlling access to community resources through role identities
- **PUC 17**: **Multi-communication**: Communication (text-based, multimedia-based) with multiple members
- **PUC 18: Organisation of ad-hoc meeting**: Locating and connecting with members
- **PUC 19: Marketing/Advertising**: Advertising service, including personalised advertisements
- **PUC 20: Real-time content sharing**: Information exchange via 'shared desk'
- **PUC 21: Enhanced social ads**: Advertisements based on member social and mobile context
- **PUC 22: Virtual marketplace**: Provisions of on-demand game related content
- **PUC 23: Advertising Service**: Advertising of potentially interesting (commercial) places

The purpose of each use case is to illustrate the role and functionality of components in delivering the stated service to the members or the operator. The choice of the nine use cases for specific attention by the architecture work is motivated by a desire to demonstrate the breadth of functionality that the PICOS community can provide. However, this choice should not be seen as an indication of the priority that the target community might place on the functionality delivered.

For each use case we describe the situation, and then 'walk through' the sequence of interactions, between member and component, or between component and component, to illustrate the process. We also include a simple reference diagram, which shows the key component required to address the situation. (Each component is shown as a box which contains all the functionalities described in the component description). The described use cases cover 30 of the 49 defined components. For those

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

components not described in the use case, their relationship with other components can be seen in the diagram included with each component description.

Some components occur in almost every use case, e.g. Event Logging, Audit and the Secure Repository. Because they provide ancillary functionality, it is easy to overlook the importance that they play in the overall architecture. It is also easy to miss that the central role that these components play can introduce a point of weakness for privacy and trust management. For example, the Event Logging components receive information that is potentially very sensitive. It is also well placed to compromise anonymity because of the ease by which links can be made between entries, and therefore partial identities and transactions. We recognise these and other risks, and will seek appropriate solutions in the implementation.

One of the most significant new use cases is the Advertising service(s), PUC 19. The functionality of these services is discussed in detail in Appendix A.

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

7.4 Target communities

We have stressed from the project's outset that PICOS is not targeting general purpose social networks, and that our technology is intended for communities that have a strong purpose and whose members have an appreciation of the need to preserve privacy and manage their identity sensibility. In addition, we are interested in communities that have a strong mobile element and require a funding model, probably based around advertising, to operate successfully.

The community aspects investigated in D2.1-2.3, and demonstrated by our three exemplary reference communities, can be regarded as representative of many communities with current or future needs for mobile services.

We have chosen to focus on the emerging field of mobile community services, which we see as increasingly important for existing communities, e.g. the Facebook 'Places' service. These services provide members with many new opportunities, but also raise new questions regarding privacy that we expect PICOS will be able to address.

At the conclusion of the project we hope to be able to show just how far our results and findings are transferrable to the more general social networks, e.g. Facebook, MySpace, etc.

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

7.5 Trust model

7.5.1 Background to trust models

Strictly speaking, trust models should not be part of an architecture document. They describe a basic requirement that would normally be explored in requirement gathering deliverables. In fact, this was the case, but the concept of trust models was unfamiliar to our reference communities. Equally, the trust that underpinned our reference communities was not 'clean and logical', and was therefore hard to capture. Therefore, we decided to use our expert knowledge to interpret the likely requirements and thus define a suitable trust model.

We began D4.1 by considering how the different community member's attitude to risk varied. Some were risk accepting, while others were risk averse.

D4.1 adopted a very specific trust model, a trust model that places greater dependency on a single entity like a community operator, but offered less privacy control to the individual. This 'high trust' trust model does not resonate well with users who are concerned about current privacy practices that social networks have adopted, although it remains the trust model that we see in our reference Angling and Gaming communities.

For those members who do worry about the risks of using a community, a range of options are possible, essentially where members take greater or lesser control of the situation according to their personal beliefs. Other members will look for assurances from the community operator. We showed that there is a spectrum of possibilities, from high trust (low personal control) to low trust (high personal control), as the following diagram shows.

Figure 11 Trust spectrum

Somewhere between these two extremes lies the community that concerns PICOS, and for the first set of prototypes we used a trust model that is exemplified by the angling community. This community is particularly interesting because it possesses the following characteristics:

- It has a well defined purpose
- Members have a shared interest and shared values
- It has a co-ordinating entity that shares the same values
- It existed in the real world

Compared to a social network community, where trust is high and personal control low, the angling community looks for a balance of increased personal control and reduced need for trust. By contrast, a highly distrusting member would, compared with today's standard community offering, look for much greater control and reduced need to trust.

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

Solving the trust challenge that we see in social networks requires a different approach. Essentially, the trust placed in the community operator is removed and distributed to one or more trust domains in a way that is acceptable to the membership. In addition, sensitive process that might otherwise be carried out within the community is now performed in an isolated (probably local, e.g. smart phone) environment that the member trusts.

Addressing trust concerns through enhanced isolation is one approach to dealing with privacy concerns. In essence, it is a strategy of data minimisation, where only essential information is ever revealed to another party. However, communities basically exist to share information, some of which is personal. To deny the community this opportunity would indeed address privacy, but it would also devalue the community experience to such an extent that it is no longer viable.

Another way to think about trust is in terms of the effectiveness of a response to abuse of trust. Management of abuse was raised in D2.4 Requirement R2.14, where penalty transactions were mentioned. Since abuse can often appear to be more significant than good behaviour, the remedial action – e.g. how PICOS offers support to members when dealing with complaints from others (Requirement R1.14).

The provision of an external connection to a community stands to undermine trust, e.g. the suggested likely interconnection with other communities as discussed in the sub-section of architecture topologies. External interfaces, a requirement that D2.4 highlighted (R4.8), are seen as a necessity of open community architectures and an important feature for building interrelationship through external services.

7.5.2 Choice of trust model for the PICOS architecture

The following figure (Figure 12) summarise this situation, and shows where the prototypes of PICOS community are focused.

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

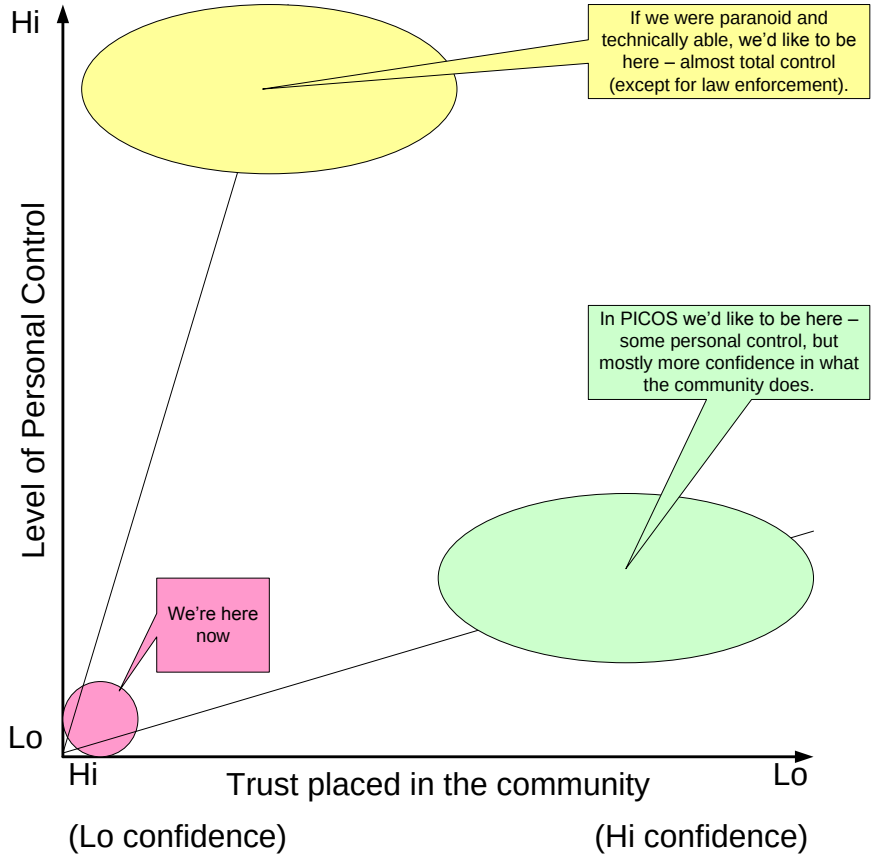


Figure 12 Balancing trust and control

We further defined the target community by stating the desires of the membership. We stated that members:

- Are interested in greater control over how their information is shared
- Want features that are not present in today's communities, e.g. Address books, groups, greater confidence in the identity of other members (OpenID, ID Brokers), evidence that their information has been accessed, assurance that the community complies with the law, a reputation system, feedback, profiles and privileges
- See the greatest threat coming from other members, not from the community operator, and from hackers outside of the community.
- Would trust a community that employs the latest (PICOS) technology to manage trust and privacy
- Believe that the community operator will be willing, or obliged (by law), to protect their data
- Do not require absolute guarantees, and consider 'after the event', or retrospective, control adequate

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

- Would not check the technology
- Use a community's reputation to decide how trustworthy it is
- Are more concerned about the authenticated identity of another member
- Look for strong authentication in certain situations, but third party endorsed identities was not a priority. However, would accept a mobile device that provides a trusted identity
- Are less concerned about integrity or provenance of content (they accept that content from an authenticated member is genuine)
- Want secure storage, but only for the more sensitive information
- Accept that law enforcement requires access to protected information, and would trust the community operator to perform the role of trusted intermediary
- In general, trust the community operator to perform the role of a trusted intermediary

In D4.1, and more so in D4.2, we contemplated a low-trust trust model, in which members do not (or at least should not) trust the community operator, as is typical of today's social network communities. Whilst we agreed that technology existed that could address all of our concerns, implementing such technology in a way that members would find acceptable was thought unlikely. Furthermore, the technical challenges that some of the more advanced privacy controls present could discourage existing community operators and providers from adopting the PICOS architecture.

For example, anonymous interaction with a community operator would require trusted intermediaries and more sophisticated processing capabilities on the client device. It would also meat the community operators know very little about their membership, which could severely limit the range of services that they can offer, and connecting 'like minded' members would be much harder. Whilst these are good measures in terms of privacy, they are at odds with current community goals around 'easily connecting people'.

For this reason, we decided that D4.2 should retain the original trust model – i.e. place high trust in the community operator – but to find alternative ways to deal with particular concerns that may arise, e.g. sharing information with third-parties and advertisers.

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

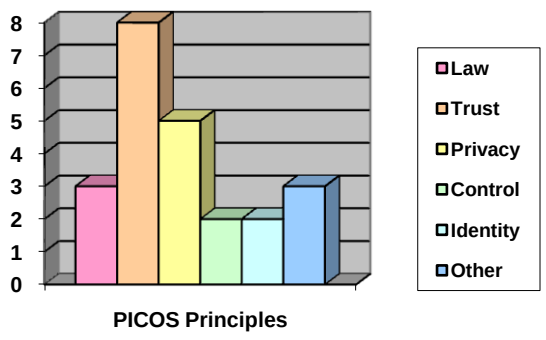
7.6 PICOS Principles

D4.1 established 23 PICOS Principles, summarised here and detailed in Appendix B. These principles continue to guide our architecture design. Each principle was derived from the requirements gathering phases of the project, and influenced by our experience in the fields of communications, security and social values in trust and privacy.

Each Principle falls into one of six key areas, namely:

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

The distribution of the 23 principles is as follows[2]:



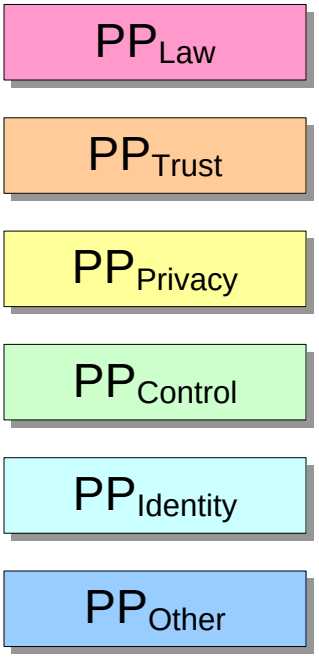


Figure 13 Distribution of principles

[2] If viewed/printed in 'black and white, the columns read from left to right: Law, Trust, Privacy, Control, Identity and Other.

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

The 23 PICOS Principles are listed in the following table (Table 4), ordered according to the main category that best describes the contribution that the principle makes to the architecture.

PP_{Law}	PP_{Trust}	$PP_{Privacy}$	$PP_{Control}$	$PP_{Identity}$	PP_{Other}
PP1: Compliance with Legislation	PP5: Openness and transparency	PP8: Data minimisation	PP3: Use of personal information	PP2: Data Ownership	PP7: Topology agnostic
PP15: Data controllers	PP6: Trust between communities	PP9: End-to-end privacy	PP4: Protection of personal information	PP11: Use of pseudonyms	PP10: Offline working
PP22: Trusted intermediary	PP12: Provenance	PP17: Authentication			PP20: Resilience
	PP13: External services	PP18: Multiple persona			
	PP14: Audit	PP19: Sub-groups			
	PP16: Objective and subjective trust				
	PP21: Diversity				
	PP23: Trust				

Table 4 Summary of principles

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

7.7 PICOS Features

7.7.1 Feature selection

D4.1 carried out a comprehensive requirements gathering exercise, notably with deliverables D2.3 and D2.4. From these we produced a short-list of key features that members of a PICOS community value most. The features were derived from our examination of all our reference communities, but in D4.1 the analysis focused heavily of this first prototype and the pressing needs of the angling community.

We began by expressing these features in terms of the benefit that they offer members. Then we described each feature in greater detail (see Appendix C), indicating the implications for an implementer of a PICOS community.

D4.2 has enhanced and extended our understanding of these features, despite no significant new features being introduced.

7.7.2 Key to features

Each feature was categorised according to the contribution that it makes to a PICOS community with respect to communities in existence today. Each was assigned an appropriate icon as follows:

PICOS$_{\text{distinguishing}}$ PICOS introduces the new community feature

PICOS$_{\text{enhancing}}$ PICOS enhances this traditional community feature

PICOS$_{\text{mobility}}$ PICOS enables mobility through this feature

7.7.3 Features most valued by members

We believed that the best way to express member requirements is in terms of what they want from their community.

Informally, community members wanted to:

- Share information (content) with other members
- Send messages to other members and, in general, have access to a range of different communication services, including real-time interactive 'instant messaging' and push-pull notification (e.g. voice/text messaging)
- Search for 1) members with similar interests and 2) information on specific topics
- Create or join sub-groups of members within the community
- Build trust in other members through the use of 1) reputation, 2) non-repudiation and 3) closed membership (registration)
- Access external services that offer additional specialist functionality

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

- Mark (tag) documents in such a way that access and use can be restricted
- Receive notifications that improve understanding about risk related to an action about to be performed
- Interact with external communities on the same basis as local community
- Have essentially the same experience whether mobile or static
- Personalise experience and expectations of the community based on particular requirements and values.

These eleven high-level features were expressed in a way that makes sense to the target membership. From this list we identified a set of system features that would need to be implemented to satisfy these higher level goals.

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

7.7.4 Main system features

The system features that satisfy the needs of a PICOS community are as follows:

Feature	Description	PICOS$_{mobility}$
1	Reputation	
2	Content sharing	✓
3	Registration	
4	Personalisation	
5	Messaging	
6	Searching	
7	Sub-communities	
8	Presence	✓
9	External services	✓
10	Content tagging	
11	Communication services	✓
12	Notification	✓
13	Inter-community interaction	
14	Mobility	✓
15	Non-repudiation	

Table 5 Summary of features

The features marked with a check mark (✓) are considered to have particular, possibly unique significance for a mobile community.

In Appendix C we examine each feature in detail, and explain how PICOS addresses the privacy and trust concerns that naturally arise.

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

7.7.5 Summary of PICOS features

PICOS$_{enhancing}$	PICOS$_{distinguishing}$
PF1: Reputation	PF10: Tagging
PF2: Content sharing	PF14: Mobility
PF3: Registration	PF15: Non-repudiation
PF4: Personalisation	
PF5: Messaging	
PF6: Searching	
PF7: Sub-communities	
PF8: Presence	
PF9: External services	
PF11: Communication services	
PF12: Notification	
PF13: Inter-community interaction	

Table 6 Distribution of features between PICSO enhancing and PICOS research

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

7.8 Economic perspective

7.8.1 Challenges and motivation

One might ask why organisations involved in marketing and advertising are interested in communities. A lot of the information that is shared within social networks[3] is very personal. Detailed user profiles describe members' personalities and interests, including for example holiday pictures and semi-public conversations with other members and across interest groups, and more publically on guest-boards.

Besides the huge numbers of users that are now registered and using community networks, the significant amount of personal time that they devote, and the detailed data about themselves and other user that they share, had made social networks increasingly attractive to marketing organisations over recent years [Hoegg, 2006] [Nielsen, 2009].

From a marketing perspective, they represent an attractive field in which to conduct targeted marketing activities, and thereby extend the classical boundaries of content related marketing. Targeted marketing activities have become more and more intensified, ranging from simple banners that are displayed based on profile attributes of users (cp. [Facebook]) to mobile reward systems for "checking in" at specific locations (e.g. cafés) [Loopt] [Foursquare] (Figure 14).

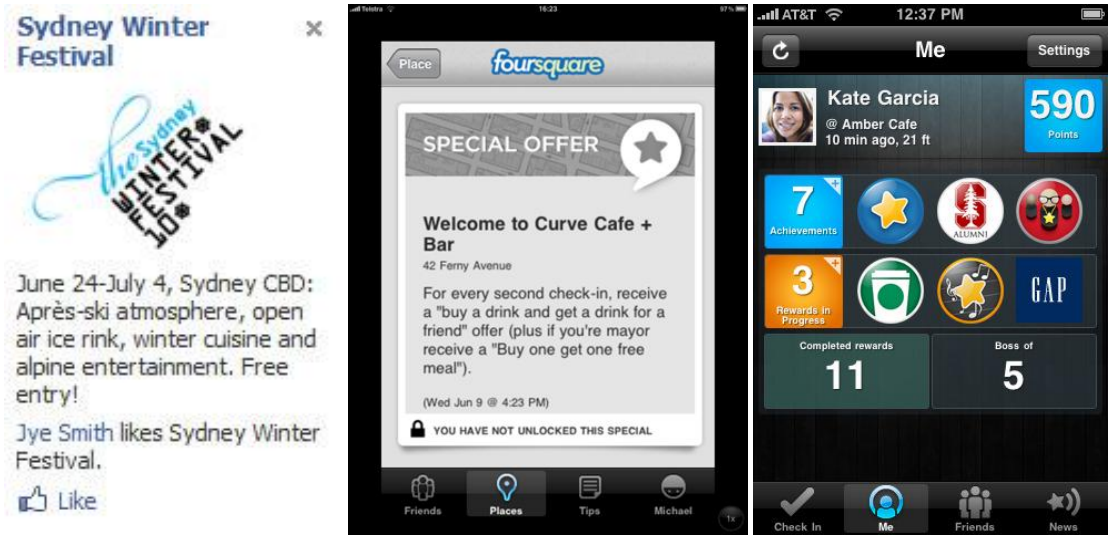


Figure 14 Social network marketing in practice (left to right): Facebook, Foursquare, Loopt Star

The Benefit of targeted Marketing activities within social networks is not only a benefit for suppliers and advertising companies, but also for social network providers (and therefore members too). Advertising, when linked to specific marketing activity, is an important means for social network providers to generate revenues and part hence an integral part of many providers' business models. On the other hand, these activities are still considered ineffective as in many cases users pay little

[3] Also referred to as "Social Communities".

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

attention to advertisements due to their attention on other activities, e.g. communication with other community members. This finding is supported in various recent studies, e.g. [Nielsen, 2009] [Linkshare, 2009] [IDC, 2008].

Editor note: In the following paragraph, and later in more detail in sub-section 9.2.1, viral marketing is promoted as a way for advertiser to easily contact a large group of otherwise unknown like-minded community members. To a certain extent, viral marketing adheres to the privacy goals of PICOS is that members remain anonymous from advertisers. However, viral marketing can also been seen as Spam, and therefore at odds with the PICOS Principles under the groupings of Trust and Control. Just as privacy respecting with reputation management, getting the balance right between protection and usefulness is not easy, and potentially challenging for privacy respecting advertising.

Social networks are particularly attractive for viral marketing campaigns. The principle of viral marketing is that marketing message are spread between users just like a virus [Kotler, Arnstrong, 2006], a principle that fits very well with communication-intensive environments like social networks [Subramani, Rajagopalan, 2003]. This is especially true when communication occurs at a personal level and comprises shared interests. Hence, content contributed to groups, walls and profiles, which then becomes share information within the social network, are used to promote products/services (e.g. video games, beverages), brands/companies (e.g. Nike, Apple), events (e.g. New York City Marathon). There is a flip-side too, where members can use the same techniques to share opinions and discuss with other users their own views about these brands, products or companies.

From the PICOS perspective, advertising is an important factor in the context of online and mobile communities [PICOS 1, 2007]. A community services platform, like that developed by PICOS, needs to recognise the potential importance of advertising based marketing, and facilitate such marketing activities recognising that in most cases these will be with 'external' third parties. The need is increasingly important for mobile activities (and consequently mobile communities), as reported in [PICOS 2, 2007].

7.8.2 Concerns about advertising in communities

However, the use of personal information for marketing and advertising purposes raises new and worrying questions regarding the privacy and protection of personal data. From the PICOS perspective one of the main questions is to what degree are users able to control for themselves the use of their personal information (cf. [Liesebach, Scherner, 2008] [Chew et al, 2009]).

This question leads to new challenges with regard to the research on privacy enhancing technologies for social networks. And given the challenge of funding social networks, and the clear benefit from a commercial perspective that advertising brings, a balance needs to be achieved between the privacy needs of users vs. the interests of the advertisers and those of the social network provider [Liesebach, Scherner, 2008].

An importance consideration is the relationships between users and their communication within the community, as emphasized repeatedly, e.g. [Duncan, Moriarty, 1998] [Palmer, Koenig-Lewis, 2009]. In [Kahl, Albers, 2010] the idea of tightly integrating marketing with user communication is suggested as an area for future research. PICOS has investigated this particular issue, and conducted research to further elaborated the concerns and options in the context of a PICOS community. Our research first extends the theoretical foundation within this deliverable, and then produces an exemplary outline showing how the integration in a real privacy–enhanced community service infrastructure can be

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

achieved. This in turn will directly influence the PICOS Gaming Community Application Prototype (D6.2).

Figure 15 contrasts traditional direct marketing with social network marketing [Palmer, Koenig-Lewis, 2009] and shows the communication that occurs between producer (supplier)/advertiser, consumer/user and community provider.

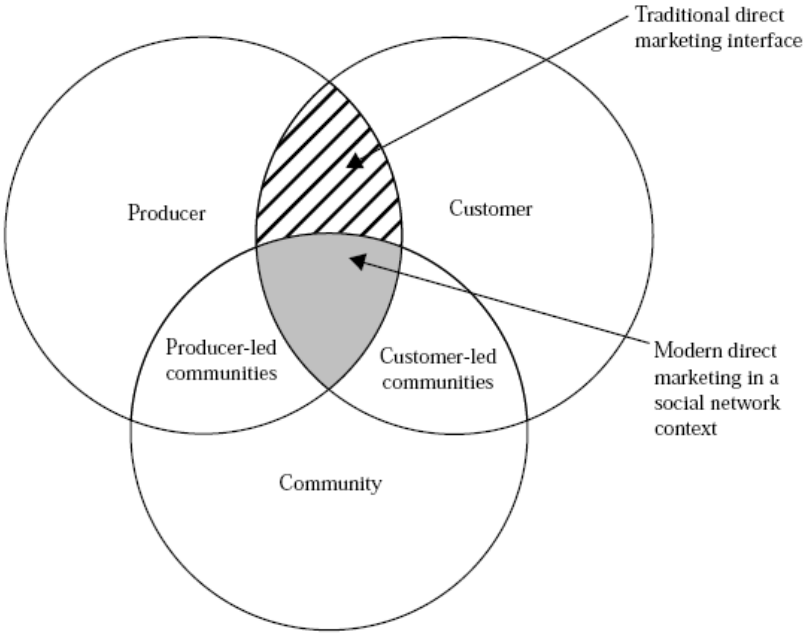


Figure 15 Traditional Direct Marketing vs. Social Network Marketing

7.8.3 Usage constraints

Advertisers face also some difficult challenges, including technical and usability, when preparing adverts for mobile environments. The constraints that exist in the mobile network and on mobile platforms hamper advertisers' creativeness, and thereby the potential for effective advertising. For example:

- Storage for data and cookies is limited in a mobile
- Communications speed and bandwidth are both issues
- Optimised data from third-party ad servers is not available
- Screen size is a very limiting factor. Given the limited space, words and images must be kept to a minimum and the layout must be clear and concise
- Content and advertising needs to be optimized to render appropriately across thousands of different type of handsets

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

- Navigation through content and interaction with ads depends on the user's level of experience
- Tolerance of users for viewing ads is low due to the small handset display.

Only by understanding what content consumers are viewing can advertisers begin to appropriately target mobile advertising. Therefore advertisers need to understand:

- What type of mobile appliance the viewer is using
- What that mobile appliance is capable of
- Which network they are connected to.
- What type of content they are choosing to view

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

7.9 Legislative perspective

The architecture needs to ensure that all potential systems developed based on it are legally compliant. It is actually the first phase for the realisation of the Privacy-by-Design model that we later refer to in this sub-section.

The elicitation of the legal perspectives of our reference communities is closely linked to the efficient function of the architecture development activity. The definition of components - at the platform design and architecture phase of the project - that ensure the legal compliance to the European privacy and data protection legislation presents significant challenges, as these components will only be fully developed and tested when a platform or a community application prototype is built later.

However, it has been a major concern of the PICOS project to embed privacy and security elements already from the design and architecture phase in order to support the necessary legally compliant infrastructure that PICOS delivers. The relevant legal framework has already been scrutinized in previous PICOS deliverables (D2.3, D2.4 and D7.1); privacy issues and in particular the processing of personal data (with the further implications regarding identity management) are taken into account at the earliest stage of the organisation of the PICOS infrastructure, i.e., the platform design and architecture, in full respect of the "privacy by design" principle, which is strongly promoted by the European Commission.

Richard Thomas, the former UK Information Commissioner has emphasised that organisations must embed privacy by design, and data protection must become a top level corporate governance issue[4]. Conducting research on the privacy and data protection issues at this early stage of the development and adoption cycle of the platform prototype will allow PICOS to have the privacy and data protection principles "built-in" in the PICOS system used in future application communities.

7.9.1 The current situation

PICOS aims at the creation of a fully legally compliant architecture and consequently platform and community application prototypes. The current legal framework on privacy, data protection and identity management has already been analysed in PICOS Deliverable D2.3 "Contextual Framework" and has been complemented with specific legal requirements contained in PICOS Deliverable D2.4 "Requirements", which assist the developers in creating a fully legally compliant architecture, while country-specific reports on the data protection and identity management related legal frameworks are included in Deliverable D7.1 "User Evaluation Plan". The legal requirements appear as principles in Appendix B of the D2.4 and serve as guidelines to the developers of the architecture.

As PICOS in an EU-funded project, the PICOS Architecture and Design is based on the relevant European legal and regulatory framework on privacy and data protection. This choice is also implied by the statement of PICOS included in the PICOS Description of Work which clearly stipulates that the "results of PICOS will contribute to European competitiveness in two ways. Firstly, the resulting platform will enable European telecommunications systems equipment suppliers to include privacy-enhancing and trust-enabling identity management features into their offerings in an interoperable manner, thus strengthening the attractiveness of these to their communication service provider

[4] UK Information Commissioner's Office (ICO), Making European data protection law fit for the 21st century (Press Release), 12 May 2009

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

customers. Secondly, the deployment, by European communication service providers, of community-supporting capabilities that enhance the privacy and trust aspects of identity management will make citizens' attitudes about participation in on-line communities more positive and confident, thereby increasing such participation and so enabling the benefits of the digital economy to be attained more than otherwise". Therefore the choice of PICOS to focus on the European legal framework is in light of its nature as an EU funded research project and it does not ignore the potential importance of other international or national (non-EU) legal frameworks that would be applicable in a potential commercial exploitation of the project results in a global implementation.

In the field of European Union law, the Charter of Fundamental Rights of the European Union (hereinafter EU Charter) provides for the respect for private and family life (Art.7) and the protection of personal data (Art.8), while the Data Protection Directive (1995/46/EC) has been adopted to guarantee efficient data protection. The PICOS project ensures compliance to the aforementioned legal framework.

Article 8 of the European Convention of Human Rights (ECHR) also protects the right to respect for private and family life. However a complaint with the European Court of Human Rights (EctHR) can only be filed in respect of violations by a State that has ratified the ECHR. Currently, the procedures set up by the ECHR do not allow its direct enforceability from individuals. A complaint against an individual or private party is "*inadmissible for reason of incompatibility with the Convention* ***ratione personae***"[5]. Such an alleged violation can be lodged at the ECtHR only indirectly, i.e., when a Member State "*can be held responsible for the violation in one way or another*"[6], for example by not providing appropriate protection against, or remedies for, a violation of Article 8 rights. Given the commercial nature of the results of the PICOS project, the provision of Article 8 is not directly applicable and is therefore not further discussed. Similarly the ePrivacy and the Data Retention Directives are not applicable to the PICOS project. Both these Directives apply to providers of publicly available electronic communications services in public communications networks, leaving outside their scope private or semi-public services, as well as information society services. The architecture reflects one of the fundamental positions of PICOS: that PICOS aims at the creation of a legally compliant platform. In all phases, from registration through to revocation, legislation is catered for.

While various components that form the overall architecture contain functionalities that enable legislation to be enforced, there is not one single part of the architecture that has sole responsibility. Instead, compliance with legislation is a design philosophy that permeates throughout the design process. The setting out of the legal requirements and their translation into clear principles for the developers at a very early stage of the PICOS project, as well as the continuous cooperation with the legal team during the designing phase of the architecture, follows the "privacy by design model". The privacy issues and in particular the processing of personal data (with the further implications regarding identity management) are taken into account at the earliest stage of the creation of the architecture.

The legal requirements, which are translated into principles in Appendix B of D2.4, could be expressed as policies, and the policies then interpreted and acted upon by each component. Equally, components could report back how effectively they have complied, and all the reports could be

[5] Van Dijk, Pieter et al., *Theory and practice of the European Convention on Human Rights* (4th edn Intersentia, Antwerpen - Oxford 2006), p. 29.
[6] Van Dijk, Pieter et al., *Theory and practice of the European Convention on Human Rights* (4th edn Intersentia, Antwerpen - Oxford 2006), p. 29.

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

collated and presented as evidence. One of the six key areas, into which the PICOS architecture principles are divided, is Law. "Compliance with legislation" (see sub-section 7.4, PP1), "Data Controllers" (see sub-section 7.4, PP2) and the "Trusted Intermediary" (see sub-section 7.4, PP3) are three PICOS architecture principles, which are classified as having direct relation to law and more specifically to the data protection legislation. This classification shall however not be considered as exclusive. Several architecture principles that fall under one of the other key areas (i.e. trust, privacy, control, identity, other) have some relevance to law.

For instance the "Data Minimisation" principle (see sub-section 7.4, PP8), which is classified under "privacy" is also a core legal principle, according to which the processing of personal data should be limited to data that are adequate, relevant and not excessive.[7] According to this principle, data controllers are obliged to store only a minimum of data sufficient to run their services. While recognising that data minimisation is a principle adopted in European law, PICOS also appreciates that data is required in order to allow a community to grow. Technical tools and Privacy-Enhancing Technologies in particular, should be available to contribute to the effective implementation of the data minimisation requirement.

Similar thoughts can be made on the "Audit" principle (see sub-section 7.4, PP14). Besides technical audits, this principle also refers to the legal/privacy audits that are needed in order to ensure compliance of the system with the data protection legislation and the relevant obligations that derive from it. Moreover two principles that ensure the exercise of control on data are the "Use of personal information" (see sub-section 7.4, PP3) and the "Protection of personal information" (see sub-section 7.4, PP4). The former relates to the control the data subjects (in most cases the users) have on their data and the latter aims at the protection of personal data, allowing the user to differentiate between non-personal data, personal data and sensitive data. The importance to differentiate between personal and sensitive data has already been highlighted in D2.3.[8]

With regard to automatic checking for compliance, automated checking of policies and regulations would be required. This represents a significant amount of research and development, on areas of new languages to universally express and process such legal restraints; security indicators to monitor infrastructures, real-time workflows to enact actions upon alerts are needed, etc. Legal compliance within PICOS developed tools and services are of paramount importance. The relevant rules are taken into account for the design of many of the core components of our architecture, especially all those dealing with identity management, privacy, reputation, content sharing, etc.

For instance the "Consent management" component (see Appendix E) is closely related with the legal provisions of the Data Protection Directive on consent. It allows the members to modify or withdraw their consent, and it invokes the community-specific procedures that are applicable when consent is withdrawn, e.g. deletion of data, change to access rights to data, restrict access to community operator role only. The relation between the "data minimisation" component (see Appendix E) and the data minimisation legal principle has already been implied above, during the discussion of the PICOS Architecture principles. The "Location sensor" component (see Appendix E) is also closely related to legislation as it provides an interface to retrieve the current location of a member. The processing of

[7] Art.6(1)(c) Data Protection Directive.

[8] Article 8 of the Data Protection Directive describes special categories of data, i.e., "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life", commonly known as sensitive data. The processing of the aforementioned data is prohibited, unless one of the specific grounds described in the same Article is fulfilled.

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

location data is allowed according to the provisions of the ePrivacy Directive, as described in the PICOS D2.4 "Requirements" deliverable. Furthermore the "Audit" and "Accountability" components (see Appendix E) deal with the compliance of the user actions with, among others, his legal obligations.

7.9.2 What this means for the PICOS architecture

PICOS needs to ensure that all personal data are kept in a form that permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[9] However, PICOS does not need to comply with the Data Retention Directive[10] and retain specific categories of data for law enforcement purposes. As it has already been discussed in PICOS D2.3 "Contextual framework" the Data Retention Directive applies only to providers of publicly available electronic communications services or public communications networks. Consequently the relevant obligations will cover only the telecommunications or mobile operator who enables some of the PICOS functionalities and not PICOS itself.

As PICOS aims at the creation of a fully legally compliant architecture, it has embedded the legal requirements into the PICOS architecture principles and the PICOS components. The setting out of the legal requirements and their translation into clear principles for the developers at a very early stage of the PICOS project, as well as the continuous cooperation with the legal team during the designing phase of the architecture, follows the "privacy by design model". Accordingly, the whole concept of the PICOS architecture, its principles and components respect the data protection legislation and takes into account the needs of the law enforcement in the future.

[9] Art.6(1)(e) Data Protection Directive.

[10] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L105, pp. 54–63 (15.03.2006).

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

7.10 Assurance perspective

Editor's note: Our assurance model for D4.2 differs from that predicted in D4.1, and is now based on threat analysis, a change agreed by PICOS partners in July 2009.) This change leads to a more pragmatic assessment of assurance than adopted by the first cycle.

Thus, D4.2 explains how the architecture defends against a set of known threats (and vulnerabilities). The set of appropriate threats is at the time of writing still being finalised, and is expected to be tightly aligned with ENISA publications that relate to social networking.

It is also noted that many ENISA requirements go beyond the privacy principles that were defined in D3.1.

7.10.1 General approach and methodology

This section begins with a brief review of the assurance metrics that earlier deliverables recorded as relevant to privacy, trust and identity management. Listed is the set of privacy principles that WP3 identified as important to providing an assurance indication.

The assessment of assurance is subdivided by:

- Safeguards

  Analysis of vulnerabilities present in the architecture, and whether an exploitable threat either now or in the future.

- Threat analysis

  Analysis of the current/future threat landscape.

- Reputation

  Analysis of threats that relate to reputation, since reputation is a dominant trust indicator.

- Testing

  An assurance assessment is in part derived form a testing phase (in addition to the assessment of the documented architecture). The architecture needs to be able to support testing.

The way in which these various elements link together to create the assurance metric is shown in Figure 16. Here, the threat, vulnerability and reputation analysis all feed into the testing schedule.

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

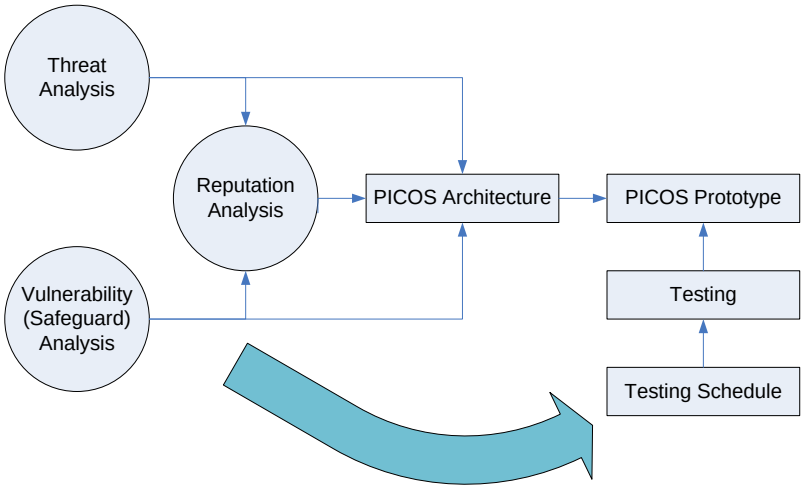


Figure 16 Assurance Methodology for D4.2

Based on the results from the first cycle assurance deliverables, D3.1.1, D3.2.1 and D3.3.1, we foresee that the assurance work for the second cycle will mainly focus on a subset of the trust and privacy principles. These include the following[11]:

- PrP01: Notice of collection (PP1)
- PrP10: Fair and lawful Means (PP1)
- PrP13: Third-party Disclosure (PP1)
- PrP17: Authentication (PP17)
- PrP18: Safeguards (PP1,PP4)
- PrP21: Data Management (PP2)
- PrP22: End-to-end Privacy (PP9)
- PrP24: Multiple Persona (PP18)
- TrP03: Provenance (PP12)
- TrP05: Audit (PP14)
- TrP06: Objective/Subjective Trust (PP16)
- TrP07: Consensus (PP21)

[11] PICOS deliverable D3.4.1 provides a comprehensive description of the PICOS Privacy Principles (PrP) and PICOS Trust Principles (TrP), and their relationships with the Privacy Principles (PP) that were used in deliverable D4.1

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

- TrP08: Accountability (PP23)

The remaining principles 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. The principle PrP18 Safeguards is particularly important at this stage, and a sub-section below is dedicated to it.

Following our assurance based development methodology described in deliverable D3.1.1, we plan for the second phase of the PICOS project to concentrate on an analysis of threats, risks and vulnerabilities concerning trust and privacy in PICOS, as well as testing. This focus may lead to a less systematic assurance description than achieved in the first cycle, but on the other hand one that is more pragmatic.

We will base our threat analysis on the threats and recommendations presented in several papers published by ENISA (European Network and Information Security Agency). Recommendations may be seen as countermeasures to known attacks. 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 will also be considered. The full list is given below:

- ENISA report on social networking and mobility

  http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens

- Security Issues and Recommendations for Online Social Networks

  http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks

- Security Issues in the Context of Authentication Using Mobile Devices

  http://www.enisa.europa.eu/act/it/eid/mobile-eid

- Reputation-based Systems: a security analysis

  http://www.enisa.europa.eu/act/it/oar/reputation-systems/reputation-based-systems-a-security-analysis

- The RISEPTIS report (relating to trust), 'Trust in the Information Society'

  https://www.tssg.org/trustandsecurity/2010/04/riseptis_report_nears_the_5000.html

- The Madrid Resolution

  www.gov.im/lib/docs/odps//madridresolutionnov09.pdf

- Spanish study on the Privacy of Personal Data and on the Security of Information in Social Networks

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

http://www.inteco.es/Security/Observatory/Publications/Studies_and_Reports/estudio_redes_sociales_en]

Finally, testing concerning privacy and trust, and particularly with relation to the detected vulnerabilities, should be part of the second cycle of the PICOS project, and a special sub-section below is dedicated to this issue.

7.10.2 Safeguards

The principle PrP18 Safeguards is especially important during the phases of prototype implementation. This principle is related not to privacy goals, but to privacy vulnerabilities, which becomes crucial at the current stage of development. Hence, a vulnerability analysis is called for. These vulnerabilities may include the following:

- Unauthorized access to personal information
  - Related to PrP13 Third-party Disclosure, and PrP21 Data Management
- Identity theft (impersonation)
  - Partially related to PrP13 Third-party Disclosure, but it is wider
  - Might affect TrP03 Provenance, and TrP08 Member Accountability
  - Possibly a new privacy principle should be included, e.g. identity
- Information Aggregation concerning partial identities
  - Related to PrP24 Multiple Persona
  - Due mainly to location and presence information, and other PID profile information(e.g. interests, relationships), information may be combined to link partial identities
- Information Storage Vulnerabilities
  - Related to PrP13 Third-Party Disclosure
  - unauthorized access to profiles (personal and sub-communities), and to auditing information
- Information Transmission Vulnerabilities
  - Related to PrP13 Third-Party Disclosure, and PrP22 End-to-End Privacy
  - Also PrP01 may be affected
  - Question: is it possible to intercept data during transmission?
  - Which mechanisms have been used in order to enforce data confidentiality during transmission?
- Information Collection Vulnerabilities
  - Is it possible to collect information, directly or indirectly, without the consent of the data subject?

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

    - Concerning content data, is it possible to collect or receive data by unfair or unlawful means?
    - Related to PrP10 Fair and Lawful Means
- Session vulnerabilities
    - How is a session maintained?
    - Is it possible to impersonate someone due to any vulnerability related to the way a session is maintained?

These vulnerabilities should be analysed in relation to the platform design architecture.

7.10.3 Threat analysis and recommendations for security

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

The following threats should be targeted:

- Digital dossier aggregation
    - How are personal profiles protected?
    - Can personal profiles be downloaded and stored by third parties
    - Can information revealed be used for purposes and in contexts different from the ones the profile owner has considered?
- Secondary data collection
    - Secondary data refers to time and length of connections, location (IP address), profiles visited, messages sent and received, and similar
    - Is it possible for third parties to collect logged data about activities performed by users?
    - Is it clear to users whether any secondary data is collected and in this case how it is used?
    - Do privacy policies refer to eventually collected secondary data?
    - Is the user informed about privacy policies concerning secondary data?
- Linkability from image metadata
    - May images be tagged, allowing unwanted linkage to personal data?
- Account deletion
    - Is it possible to remove secondary information linked to a profile such as public comments?
- Spam
    - Is it possible to receive unsolicited messages? May those be blocked?

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

- Cross site scripting, viruses and worms
  - Is PICOS vulnerable to cross site scripting attacks and threats originating from widgets from third parties?

An answer should also be given concerning the following recommendations:

- 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.
- Stronger authentication
  - Stronger authentication and access control should be used in certain social network environments; CAPTCHAs could be also used.
- 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.
- Default settings should be made as safe as possible.
- Deletion of 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.
- Encourage the use of reputation techniques.
- Filtering
  - Build in automated filters. Offensive, litigious or illegal content should be blocked by smart filters.
- 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.
- Spidering and bulk downloads
  - Restrict spidering and bulk downloads. Operators should protect all means to access profiles which might lend themselves to bulk access. Access restrictions should also be put in place to make it harder to create bogus accounts.
- Search results

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

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

7.10.4 Reputation

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

The main threats to the reputation system are the following:

- 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.
- Sybil attack
    - The attacker creates multiple identities (sybils) and exploits them in order to manipulate a reputation score. It is important to analyse whether the notion of partial identity in PICOS prevents or facilitates sibyl attacks.
- 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.
- Bootstrap issues
    - This issue is related to the initial reputation value and the choice of the entry value.
- 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

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

quality assurance. Those mechanisms should therefore be put in place, and data quality should be assured.

- 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.
- Bad stuffing and bad mouthing
  - A number of users may agree to give positive or negative feedback to one entity. A proposed countermeasure is „controlled anonymity." It would be interesting to analyse this threat in the light of the partial identity concept in PICOS.
- Repudiation of Data
  - A user can deny the existence of data for which he was responsible. Logging of transactions may be used against this.
- 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 votes, or using only voters from a trusted social network.
- 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. It would be interesting to analyse how the notion of partial identity in PICOS mitigates linkability.
- Risk of Herd behaviour and Penalisation of Innovative, Controversial Opinions
  - Innovative opinions may lead to bad reputation, at least initially, and penalise creative thought. Countermeasures include allowing the computation of personalised reputation scores by means of local trust metrics. The notion of partial identity may be an important mechanism for reducing this threat.
- 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.
- Threats to Ratings
  - These threats include threats against the secure storage of reputation ratings, against the privacy of voters, against the metrics used by the system to calculate the aggregate reputation, and the reputation scoring itself.

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

Security requirements for reputation systems include the following:

- Usability/Transparency aspects
  - How transparent is the reputation system to users?
  - Can the reputation be customized by a user?
  - Are users offered qualitative assessment of reputation?
- Is an open description of the reputation metrics available to users?
  - It should be easy to report on inappropriate content, profile squatting, identity theft, and inappropriate behaviour
- Availability
  - Important when the reputation system becomes critical to the functioning of the overall system
- 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.
- Entity authentication an access control
  - Identity management mechanisms need to be in place to mitigate the risks related to identity change like sibyl attacks.
- Privacy/Anonymity/Unlinkability
  - Privacy should be preserved. The use of partial identities should be analysed in this context.
- 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
- Accountability
  - Each peer should be accountable in making reputation assessments.
- 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.
- 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.
- Verifiability

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

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

Recommendations to designers of reputation systems include the following:

- Perform a threat analysis of the reputation system
    - A threat analysis should be performed before designing or adopting a reputation system, and the security requirements should be identified. The threats need to be considered in the context of the particular application or use case.
- Develop reputation systems which respect privacy requirements
    - Anonymity would increase the accuracy of the reputation system. A more privacy-respecting design of reputation systems is needed, while at the same time preserving trust. There are mechanisms providing privacy for voters and reputation owners that can be implemented by making reputation systems interoperable with privacy-enhancing identity management systems which assist users in choosing pseudonyms. The partial identity concept user in PICOS should be analysed in the light of these recommendations.
- Provide open descriptions of metrics
    - Reputation metrics should be open and easily accessible. Threat analysis should be performed to assess whether a metric addresses all the security requirements.
- 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.
- 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.
- 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.

In general, the trust aspects of the partial identity scheme adopted in PICOS should be analysed in the light of the mentioned threats and recommendations.

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

7.10.5 Testing

Testing concerning privacy and trust, and particularly with regard to the vulnerabilities presented above, should also be part of the second cycle of the PICOS project. The objective of testing in PICOS should be to build trust and increase the confidence that the software is correct with regard to the privacy and trust principles, and that the safeguards are adequate. The idea is to discover vulnerabilities, assess their importance, and propose suitable countermeasures.

Testing is possible for the design phase of a system, and in fact should be started at an early stage, although in this case its rigor depends on the form in which the requirements and design specifications are documented. However, a more realistic approach would be to perform the following activities:

- Test requirements (possible if requirements are expressed as use cases)
- Check consistency between design and requirements specification
- Evaluate the software architecture with regard to trust and privacy

We should concentrate on the reduced set of trust and privacy principles shown above. A qualitative assessment is the most feasible approach here. However, if components and their interactions are provided in enough detail, scenarios could also be generated focusing on trust and privacy issues, and the design could be evaluated with regard to how well these scenarios are handled. Design walkthroughs and inspections can be performed in order to trace elements from the requirements specification to the components and other elements of the design, as far as there is a clear document. Verification techniques and formal checks might be performed depending on how formal the design is specified.

7.10.6 What this means for the PICOS architecture

Assurance is intended to be an integral constituent of the PICOS solution and be pursued in a holistic manner. Threat and vulnerability analysis, as well as testing, are considered to be security best practice, and can be regarded as a necessary procedure to this end. The main purpose of this analysis is to give input to the design with respect to possible threats and attacks, and in this way to help ensuring that the PICOS platform architecture and design are accurate with respect to the trust and privacy technical objectives planned. In addition, the ongoing assurance review by WP3 will provide an independent verification that the trust and privacy requirements are being adequately considered and met.

Assurance must provide evidence that the number of vulnerabilities in a software, including the presence of features that may be intentionally exploited by malicious agents, are reduced to such a degree that it justifies a certain amount of confidence that the security properties of the software meet the established security requirements, and that the degree of uncertainty involved has been reduced. The focus here is on the minimisation of vulnerabilities, since there can never be absolute certainty that these have been fully eliminated. The use of good security and privacy engineering practices and development methods is seen as an important assurance element that limits the number of flaws and omissions, and increases confidence that the requirements are fulfilled by the implemented system.

As a result of this work, there will be an increased confidence that the resulting architecture design will be able to meet the main objectives of the project, and will also be in a form that is suitable for implementation.

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

7.11 Stakeholders

In this sub-section we list the groups that have influenced our architecture design, and state what influence they had.

7.11.1 Existing information sources

Since this deliverable is the successor to D4.1, D4.1 is a central source of guidance. Similarly, the platform prototype described in D5.1 and the applications prototype described in D6.1 set expectations for what D4.2 should deliver, as does the Assurance deliverable D3.1.1. The requirements stated in the earlier deliverables, notably D2.4 and 2.6 must be fulfilled.

7.11.2 D2.6 Requirements

The process for gathering community requirements needs to be completed at a very detailed level, with the full support of experienced members of the targeted communities. Members' feedback must be taken into account during both the development and testing phases of the prototype.

The role of experienced members of communities is crucial to create a good quality list of requirements. Therefore, included in the set of members providing requirements should be several very experienced members as well as new members. To ensure good communication with community members, a single point of contact within the project team who has a direct experience with the community is identified.

The process for gathering requirements from members involves questionnaires and face-to-face interviews. Members elaborate their feedback by considering use cases and the PICOS objectives. These requirements provide a sound grounding on which to start the processes of creating the PICOS architecture.

7.11.3 Users

Requirements derived from the Angler and Gamer communities, i.e. those who make use of the platform's core functionality. Requirements specifically identified in deliverable D7.2 are of significant relevance to the architecture

7.11.4 Reviewers

- Project Officer and EC Reviewers: fulfilment of project goals with regard to privacy, identity, trust, and consistency of architecture and documentation
- Internal Reviewer, principally work packages WP3 and WP8

7.11.5 Developer community

- Developers of the platform (D5.x)
- Developers of the client (D6.x)
- Operator, System Administrator

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

7.11.6 PICOS partners

The succession of fruitful 'brainstorms' that occurs at general meetings and WP meetings has provided a rich pool of innovative ideas and suggestions. Every contributor has high expectations for what the architecture will deliver.

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

8 Architectural views

8.1 Overview of architecture description based on views

For D4.2 we have chosen to use model views to explain the architecture. The most common view model is the 4+1 view model of Kruchten [Kruchten, 1995]. Here, the '+1 view' refers to scenarios (and potentially also use cases), which help understand the alignment between other views.

This approach of using views, or view points, also helps explain the architecture from the perspective of the customer/end-user, the designer and the creator (Figure 17).

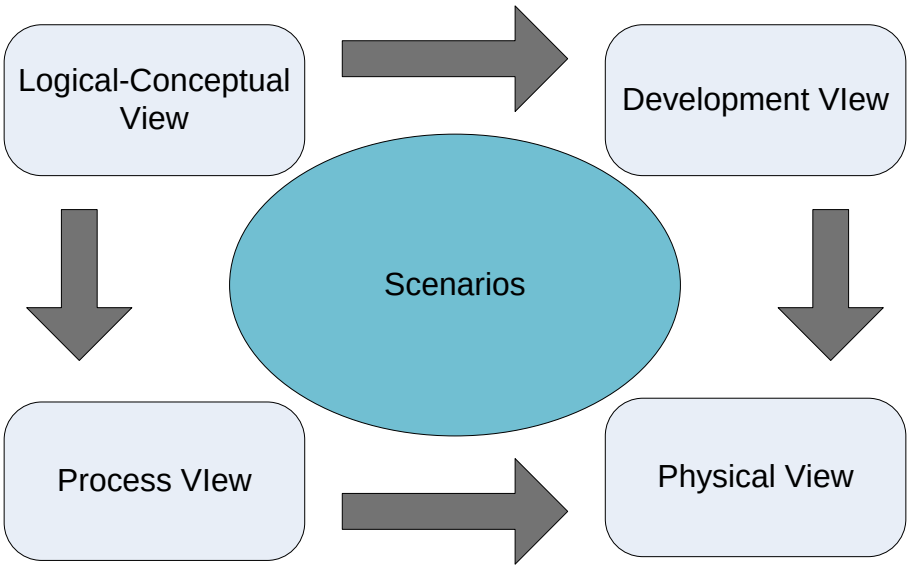


Figure 17 Kruchten 4+1 Architectural View Model

For PICOS we have slightly adapted the model by changing the description of the views, as shown in Table 7 below.

Kruchten	PICOS
Development View	Building Block View
Physical View	Deployment View
Logical-conceptual View	Trust, Privacy and IdM View
Process View	*PICOS Use Cases*

Table 7 Mapping from Kruchten to PICOS view model

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

Whilst the mapping from Local-conceptual View to Trust, Privacy and IdM View is slightly unusual, we justify the action on the basis that both describe core internal/external functionality.

Similarly, we map Process View to the set of PICOS use cases since their common ground is processes, activities and workflows (Figure 18).

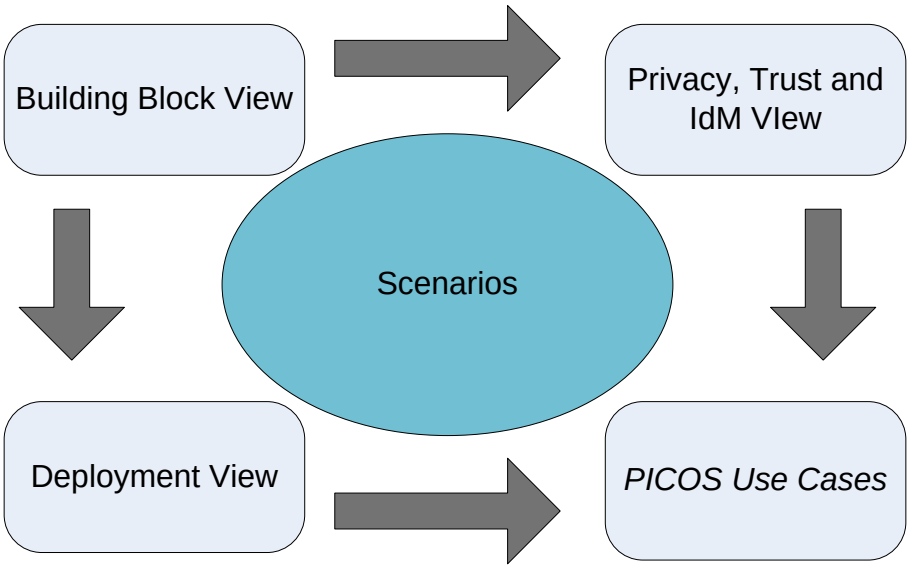


Figure 18 PICOS Architectural View Model

In the remainder of this sub-section we describe the three main views formally, before moving on to a more details description in sub-sections 8.2, 8.3 and 8.4.

8.1.1 Building Block View

The Building Block View describes how the components of the system and their relationships achieve their stated functionality. Starting with the highest level of the architecture, typically 5-10 core components are carefully selected and appropriately named. In so doing, the interdependencies of each of these components should be considered. Referring back to D4.1, this top level corresponds nicely to the component that we grouped at tier-0.

Moving down from this top level – views generally support a top down design methodology - we refine the views by specifying sub-components (the tier-1 components of D4.1 and/or components of D5.1/D6.1). We also provide mappings between the main components and this sub level, taking care to document the relationships.

8.1.2 Deployment View

The Deployment View described the distribution of the components between mobile appliance and the service provider (back-end system), and in so doing describes the additional components that help realize the connection between the distributed parts of the system. In D4.1 we describe the Deployment View in the sub-section entitled Community Topologies. An example of a deployment diagram is shown in Figure 19 below.

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

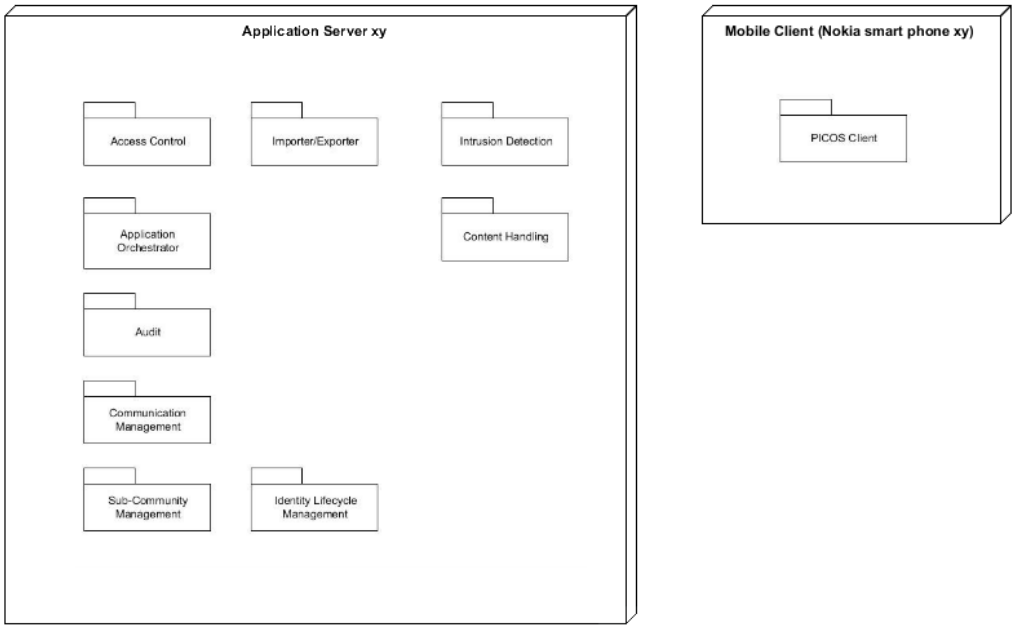


Figure 19 PICOS deployment diagram

When describing how an architecture is deployed, it is tempting to consider different infrastructure configurations. In D4.1 we announced that the PICOS architecture should be topology agnostic, a view we still hold in D4.2. For this reason we describe only one deployment view; we believe that at a practical level each topology scenarios that we discuss can be addressed by this single view.

8.1.3 Privacy, Trust and IdM View

The Privacy, Trust & IdM View describes the non-functional (privacy, trust and IdM) aspects, e.g. "what happens when a member wants to transfer content to another member. (By way of an example, in D4.1, this action involved the Policy Manager, Privacy Advisor and Sub-community Manager.) Since most components have some involvement with privacy, trust and IdM, the correlation between the Building Block View and the Privacy, Trust & IdM View in particularly strong.

8.1.4 Translating D4.1 into a view-based description

The presentation of D4.1 concepts and D4.2 enhancements according to the view model approach involved the following:

- Identification of D4.1 and D5.1/D6.1top-level components, and transfer of the components of D4.1 to the PICOS View Model. As part of this step, components roles and descriptions and were analysed, including divergence between D4.1 and D5.1/D6.1, and where appropriate refined.
- Re-assessment of the relationships between components at the top level, including alignment between D4.1 and D5.1/D6.1. Recording of the role that each component fulfils

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

- Assessment of which requirements have not been implemented, and the selection of requirements that should be implemented by D4.2 (this is recorded in D4.2 under prototype sub-section). Development and documentation of components that implement the selected requirements, including specification and documentation of the relationships between components and between these components and the other components of the architecture
- Adaptation of Use Cases from D4.1, where necessary incorporating additional/new use cases and scenarios (particularly where these relate to privacy, trust and identity management aspects)
- Creation of the Deployment View from the D4.1 description of community topologies
- Linking of requirements to components, noting that components often fulfil multiple roles and that mappings can become complex to describe. Similarly, linking components with PICOS features and PICOS principles.

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

8.2 Building Block View

In D4.1 we described approximately 50 components that contributed to the PICOS architecture. Since D4.1 was delivered, some of these components have undergone refinement. A small number of new components have also been added. In this sub-section we explain the changes that have occurred since completing D4.1. In the Appendix we describe all current components, following the same presentation style as we did in D4.1. For clarity we have introduced a new icon to highlight where a change exists relative to D4.1.

PICOS D4.2 new/updated component

Several of the new components arise due to privacy and trust requirements that emerged as we considered additional application or situations in which the PICOS might be deployed. For example, we investigate how PICOS communities might be foundered, and that led us to advertising. We also researched privacy with regard to location information, and that led us to *points of interest* and new scenarios that suited the Privacy Advisor.

D4.2 also addresses the economic aspect of a PICOS architecture. Economics did not have a strong bearing on the first architecture, but is more influential in this revision. The background to the economics perspective was discussed in sub-section 7.9. In this sub-section we describe how economics – essentially advertising – is handled at a technical level.

Before reviewing the advertising components, we first re-examine the components presented in D4.1.

8.2.1 PICOS Components

Introduction

Forty-nine actual components were identified in D4.1 from the requirements gathering stages (as reported in D2.4) of the project, which are believed to be necessary to create the PICOS architecture. Each component is categorised according to one of five broad component headings, namely:

- Services and Applications
- Content Handling
- Member Administration
- Communication
- Audit, Control and Reporting

The five component groupings lead to a simple model for representing the organisation of the PICOS architecture, which we call the PICOS 5-layer Architecture Model (Figure 20).

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

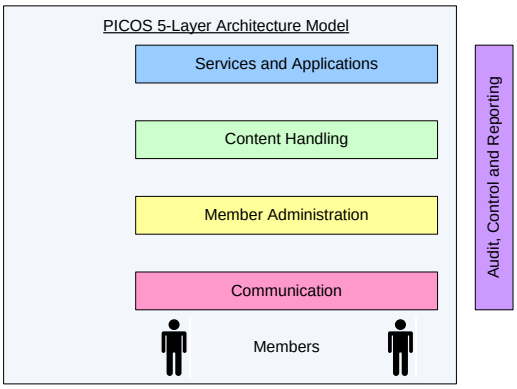


Figure 20 PICOS 5-Layer Architecture Model

Components are assigned to 'tiers'. In D4.1 we referred to the component groupings as Tier-0 functionality. We have subsequently decided to move to a two tier model, where Tier-0 simply provides a grouping capability. The term Tier-0 is therefore dropped from D4.2.

Individual components are described as either Tier-1 or Tier-2, depending on the breadth of functionality that they offer. In general, where a component relies on one or more other components for most of its functionality, i.e. the component coordinates interaction with other (subservient) components, or provides a coordinating function, is called a Tier-1 component. The subservient components are referred to as Tier-2.

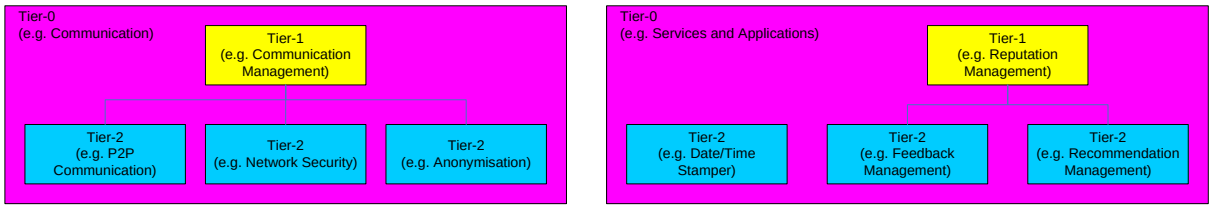


Figure 21 Example of component Tiers

In this sub-section we present the purpose and description of each component, and show the 'first level' relationship (inter-dependency) between components.

Note that we do not show every connection to every component. In particular we do not show connections to components where it is obvious from the context that such a connection would exist in practice, e.g. to the Event Logging and Audit components.

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

Component categories

As previously mentioned, each component is categorised as either Tier-1 or Tier-2. In addition, each component is categorised, and assigned an appropriate icon, according to the contribution that it makes to a PICOS community with respect to communities in existence today. Components that represent a research opportunity for PICOS are also highlighted.

T_1

Tier 1 Component

T_2

Tier 2 Component

$PICOS_{distinguishing}$

PICOS introduces the new community component

$PICOS_{enhancing}$

PICOS enhances this traditional community component

$PICOS_{research}$

Research within PICOS required. (Components requiring research are unlikely to figure strongly in the first prototype.)

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

Overview of PICOS component by contribution

The following table lists the complete set of components. Full descriptions of each component are given in Appendix A.

Title	T	$PICOS_{enhancing}$	$PICOS_{distinguishing}$	$PICOS_{research}$	$PICOS_{D4.2\ new/updated\ component}$
Access Control	1	✓	✓		
Application Orchestrator	1		✓		
Audit	1	✓			
Communication Management	1				
Identity Lifecycle Management	1	✓			
Importer/Exporter	1	✓			
Intrusion Detection	1	✓			
Preparation Area	1		✓		
Sub-community Management	1	✓			✓
Accountability	2		✓	✓	
Advertising Service	2	✓			✓
Alarms	2	✓			✓
Anonymisation	2		✓		
Archive Chat	2	✓			✓
Authentication	2	✓	✓		
Authentication Method Selection	2	✓			
Authorisation	2	✓	✓		
Consent Management	2		✓		
Contacts Management	2	✓			✓
Content Sharing	2	✓	✓		

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

Title	T	PICOS$_{enhancing}$	PICOS$_{distinguishing}$	PICOS$_{research}$	PICOS$_{D4.2\ new/updated\ component}$
Cryptography / Key Management	2	✓			
Data Minimisation	2		✓	✓	
Date/Time Stamper	2				
Delegation	2	✓			
DRM	2	✓			
Event Logging	2	✓			
Event Reconstruction	2		✓		
External Recommendation	2		✓	✓	
External Service Delivery	2	✓			
Feedback Management	2		✓		
Identity Translator	2		✓		
Linkability	2		✓	✓	
Location Base Services	2	✓			✓
Location Sensor	2	✓			
Network Security	2	✓			
Non-repudiation	2	✓			
Notification	2	✓			
P2P Communication	2	✓			
Partial Identity Management	2		✓	✓	
Payment Services	2	✓			
Policy Management	2		✓	✓	✓
Privacy Advisor	2		✓	✓	✓

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

Title	T	PICOS$_{enhancing}$	PICOS$_{distinguishing}$	PICOS$_{research}$	PICOS$_{D4.2\ new/updated\ component}$
Privilege Management	2	✓			
Profile Management	2		✓		
Public Community	2	✓			✓
Recruitment	2		✓		
Registration	2	✓			
Reputation Management	2	✓		✓	
Revocation	2	✓			
Scenario Management	2		✓		
Secure Repository	2	✓			✓
Service Selection	2	✓			
Share Desk	2	✓			✓
Social Presence	2		✓		
Trust Negotiation	2		✓	✓	
TTP Management	2	✓			
User Availability Calendar	2	✓			✓

Table 8 Overview of PICOS components

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

Component grouping

At the highest level, components are assigned to one of the 5 level of the architecture (in D4.1 referred to Tier-0 components), covering Services and Applications, Content Handling, Member Administration, Communication, and Audit, Control and Reporting.

Services and Applications Tier-1 - Subcomponents	Component Description
Access Control	Appendix E, E4
Anonymisation	Appendix E, E5
Application Orchestrator	Appendix E, E6
Authentication	Appendix E, E7
Authorisation	Appendix E, E8
Date/Time Stamper	Appendix E, E9
External Recommendation	Appendix E, E10
External Service Delivery	Appendix E, E11
Feedback Management	Appendix E, E12
Identity Translator	Appendix E, E13
Importer/Exporter	Appendix E, E14
Location Sensor	Appendix E, E15
Notification	Appendix E, E16
Partial Identity Management	Appendix E, E17
Payment Services	Appendix E, E18
Preparation Area	Appendix E, E19
Privacy Advisor	Appendix E, E20
Recruitment	Appendix E, E21
Reputation Management	Appendix E, E22
Scenario Management	Appendix E, E23
Service Selection	Appendix E, E24
Social Presence	Appendix E, E25
Trust Negotiation	Appendix E, E26
TTP Management	Appendix E, E27

Content Handling	Component Decryption

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

Tier 1 Subcomponents	
Advertising Services	Appendix E, E54
Alarms	Appendix E, E55
Archive Chat	Appendix E, E57
Contacts Management	Appendix E, E50
Content Sharing	Appendix E, E44
Data Minimisation	Appendix E, E45
DRM	Appendix E, E46
Linkability	Appendix E, E47
Location Based Services	Appendix E, E15
Non-repudiation	Appendix E, E48
Public Community	Appendix E, E51
Secure Repository	Appendix E, E49
Share Desk	Appendix E, E52
User Availability Calendar	Appendix E, E56

Member Administration Tier-1Subcomponents	Component Description
Authentication Method Selection	Appendix E, E34
Consent Management	Appendix E, E35
Cryptography / Key Management	Appendix E, E36
Delegation	Appendix E, E37
Identity Lifecycle Management	Appendix E, E38
Privilege Management	Appendix E, E39
Profile Management	Appendix E, E40
Registration	Appendix E, E41
Revocation	Appendix E, E42
Sub-Community Management	Appendix E, E43

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

Communication Tier 1 Subcomponents	Component Description
Communication Management	Appendix E, E1
Network Security	Appendix E, E2
P2P Communication	Appendix E, E3

Audit, Control and Reporting Tier 1 Subcomponents	Component Description
Accountability	Appendix E, E28
Audit	Appendix E, E29
Event Logging	Appendix E, E30
Event Reconstruction	Appendix E, E31
Intrusion Detection	Appendix E, E32
Policy Management	Appendix E, E33

Table 9 Component grouping by Tier

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

8.3 Deployment View

8.3.1 Topologies

When we began designing the PICOS architecture in D4.1, the intention was that it would by topology *agnostic*. Put another way, we envisaged a design that could be implemented easily across a range of interconnecting configurations.

The prototype that followed D4.1, by necessity adopted a very specific configuration, and though the aim is for the architecture to be flexible, the reality is that the decision would influence the ongoing development of the architecture. Specifically, this meant that the architecture would lean towards a client-server topology.

Nevertheless, it is still useful to reflect on the likely topologies that PICOS might have supported. In particular, the opportunity to explore topologies in more detail, with specific regard to privacy and trust issues that different topologies give rise to, is considered in D4.2, in relation to different trust models.

PICOS functionality is delivered as a service. Services can be hosted locally or centrally, and can be for the direct benefit of the member or of the community as a whole. As we continued to develop our understanding of the needs of a typical PICOS community, our earlier predictions that services could be grouped in terms of *personal*, *membership* and *community-generic* – in D4.1 we used the terms My Services, Our Services and Community Services respectively – became evermore apparent.

Drawing on our earlier work, the topology that best meets the needs of our reference communities is the client-server model. Currently, extensive processing at the client is not feasible, and according to the trust model that our reference communities already adopt, a centralised (and trusted) controlling authority is accepted, and from a pragmatic point of view easiest for PICOS to align with.

8.3.1.1 Client-server model

In this topology, which adopts a client-sever topology, clients (e.g. smart phones) are represented by the inner circles that host 'local' services. The client can process local service but relies on the community for shared services and services that are too demanding (in terms of computing and storage resources) for the client to host (Figure 22).

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

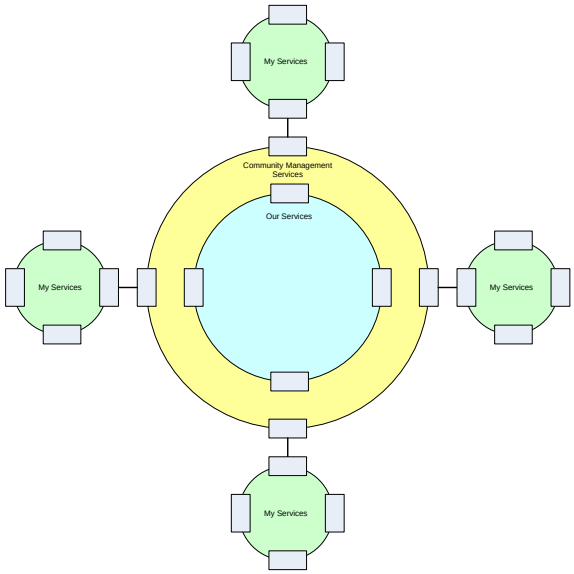


Figure 22 Client-server model

To give an idea of how such an idealised model might be implemented, we include the following figure which shows a typical mobile community (Figure 23).

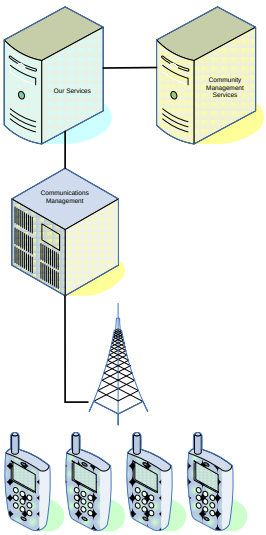


Figure 23 Client-server implementation

As demonstrated in D4.1, this simple model can easily be extended to accommodate inter-linked communities and external community service providers.

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

8.3.1.2 Client-server architecture – conjoined communities

Communities that wish to interact with one another can be arranged as shown in Figure 24. Here, two PICOS communities are interconnected, meaning that member and community services can be shared across the two communities.

Inter-community trust is a feature that the Requirements 1 (R1) review rated as important (Requirement R1.2). The justification for this is simply that people are often members of several communities simultaneously. Managing this trust can become a complex issue; Requirement R3.18 Import and Export of Credentials raised this very point.

It was proposed that that one community would provide services for the other, for example where one community is able to offer specialised features for the combined membership (Figure 24).

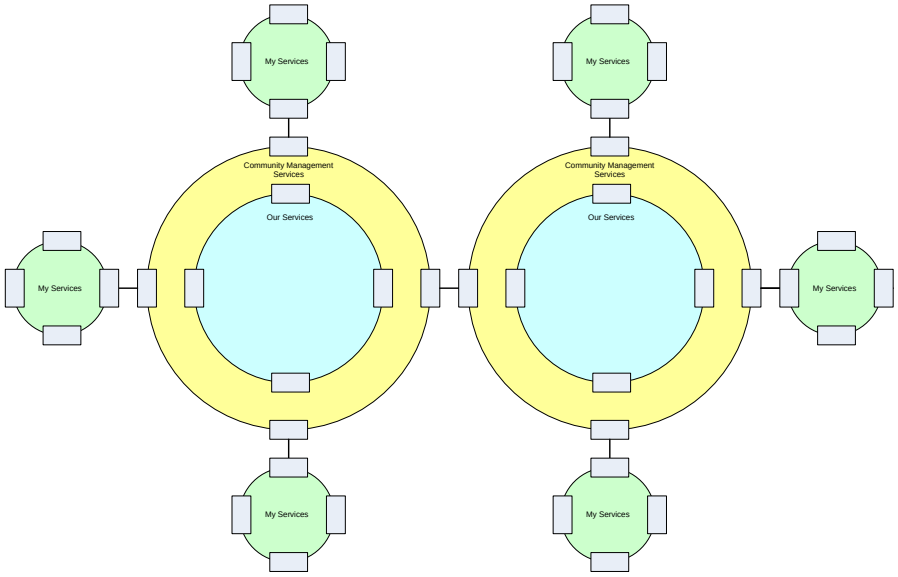


Figure 24 Conjoined communities

Similarly, some services might be provided by independent third parties, which do not have any members themselves. Such a situation might look like that shown in Figure 25.

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

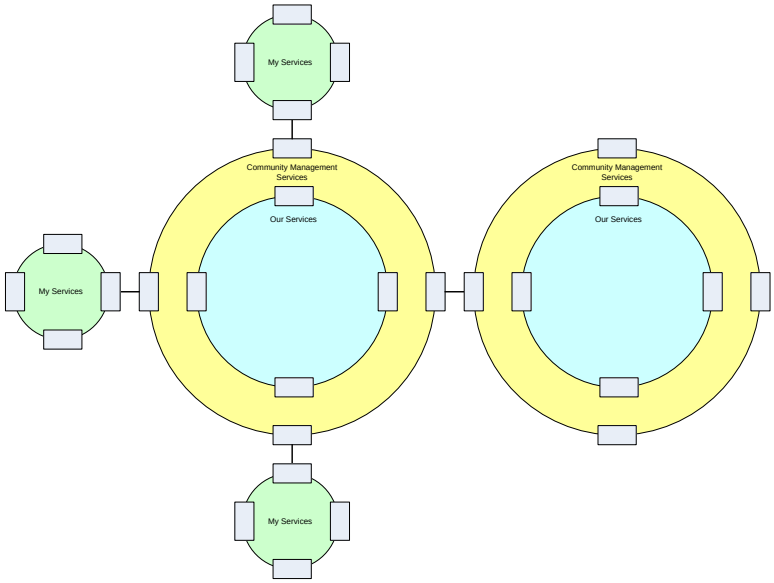


Figure 25 External services

8.3.1.3 Peer-2-Peer architecture

The second topology that we considered in D4.1 was the peer-to-peer (P2P). This model has not been fully investigated in PICOS, mainly because the trust model that it supports was not considered a good fit for our reference communities. The *transitive* nature of trust means that when communities are large, trust established using peer-to-peer relationships is unlikely to be sufficiently 'powerful'. This point was discussed in Requirement R1.8.

However, the P2P model illustrates a useful extension to the previously discussed topologies that PICOS could be architected to support.

In this model, all services are distributed amongst members, and there is no need for a trusted service provider that might otherwise host service that roves personal information. Services are shared between members, with perhaps member who have more powerful mobile appliance running the more process intensive services.

This model is particularly attractive for members who feel uneasy about trusting an unknown community operator.

It is also worth noting that P2P service can be provided 'through' a centralised community service provider. This approach closely resembles the centrally managed communications architecture that service providers, and most mobile network providers, use today. In this regard it may be seen as a more easily accepted topology since it allows a community to be built on top of conventional communication technologies network. The arrangement that extends our three tier topology is shown Figure 26.

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

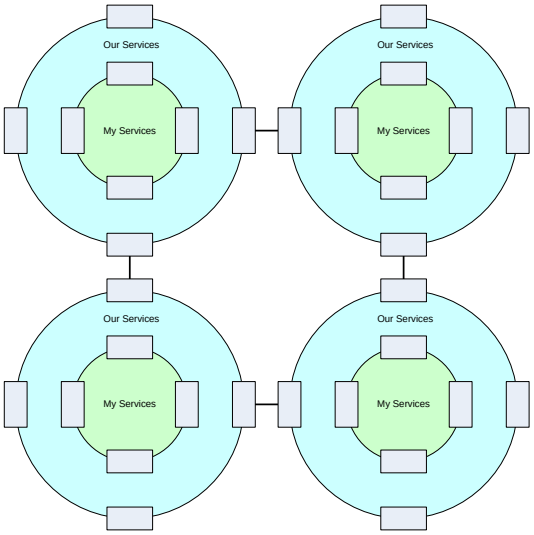


Figure 26 P2P topology

Our aim has been to look beyond the popular implementation of communities, which tend to mimic communications topologies. There are two reasons for taking this approach:

- In the near future we anticipate personal networks becoming more common. The reference communities that we have examined could benefit from such technology, for at least part of their community services. For example, anglers might form a local ad hoc community while fishing.
- Different topologies create and address different trust models. For example, P2P (no community operator) may appeal to members who trust teach other, but not a central authority. We saw this with our Taxi Driver community, where drivers had a high degree of trust in each other (formed in the real world) and saw no need to trust anyone else.

Different topologies present interesting research challenges, and some of which have been investigated by PICOS.

Finally, in D4.1 we considered the situation in which the mobile appliance has very little processing capability. We called this the *dumb terminal architecture*. It also followed our three tier topology, but was not pursued further in the project. For completeness, it is described briefly in the Appendix.

8.3.2 Single-view topology

The Deployment View described the distribution of the components between mobile appliance and the service provider (back-end system), and in so doing describes the additional components that help realize the connection between the distributed parts of the system. In 4.1 we describe the Deployment View in the sub-section entitled Community Topologies.

When describing how an architecture is deployed, it is tempting to consider different infrastructure configurations. In D4.1 we announced that the PICOS architecture should be topology agnostic, a view we still hold in D4.2. For this reason we describe only one deployment view; we believe that at a

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

practical level each topology scenarios that we discuss can be addressed by this single view (Figure 27).

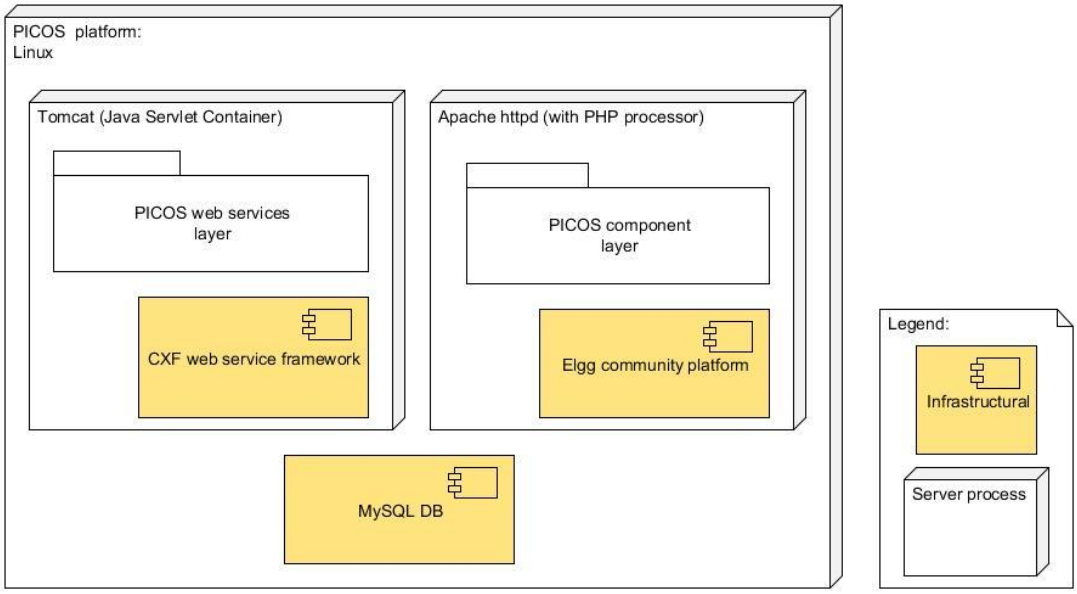


Figure 27 Single View Topology

8.3.3 Infrastructure context

Interaction of the PICOS architecture – specifically, the PICOS platform – with neighbouring systems is represented in the following three figures. A detailed description of their operation can be found in the platform prototype documentation produced by WP5. The figures are included here to give an impression of how the interactions that take place at component level, interface with the wider world.

Interaction of the PICOS architecture – specifically, the PICOS platform – with neighbouring systems is represented in the following three figures.

Figure 28 depicts the environment surrounding the PICOS platform (as implemented by WP5), including PICOS artefacts and third-party components.

Figure 29 is a schematic overview of the overall architecture, demonstrating the layered structure. Forsaking completeness, only the WP5 components are shown in this diagram.

Figure 30 shows the PICOS platform itself with its related PICOS artefacts, revealing how they are deployed across the different infrastructural components.

The figures are included here to give an impression of how the interactions that take place at component level, interface with other the wider world. A detailed description of their operation can be found in the platform prototype documentation produced by WP5.

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

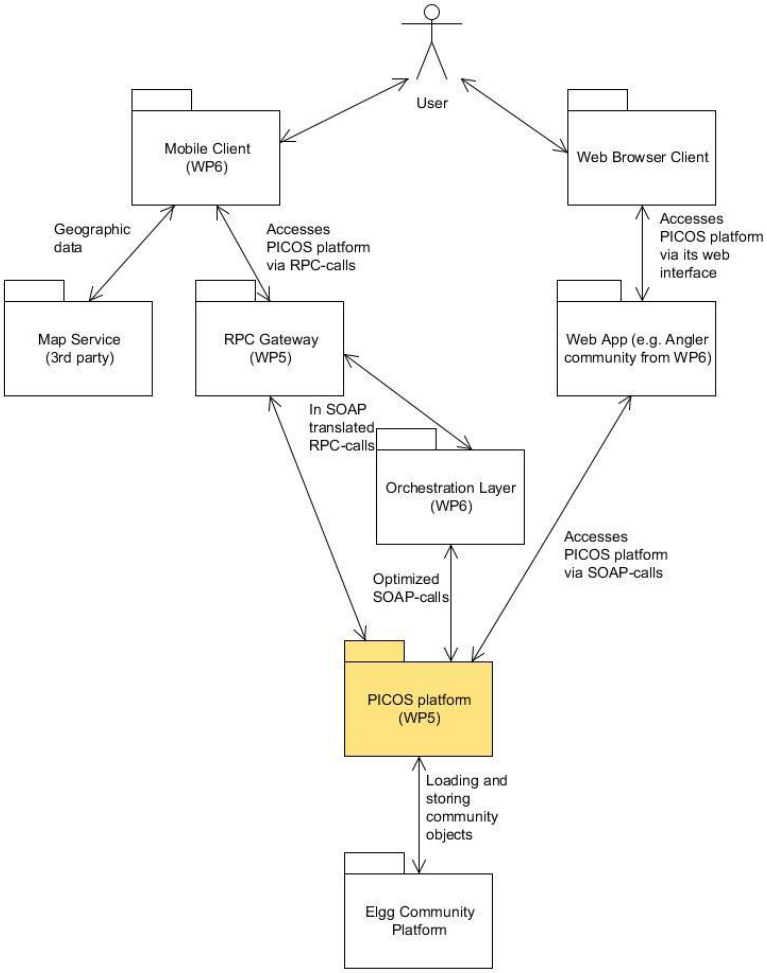


Figure 28 Infrastructure context - UML

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

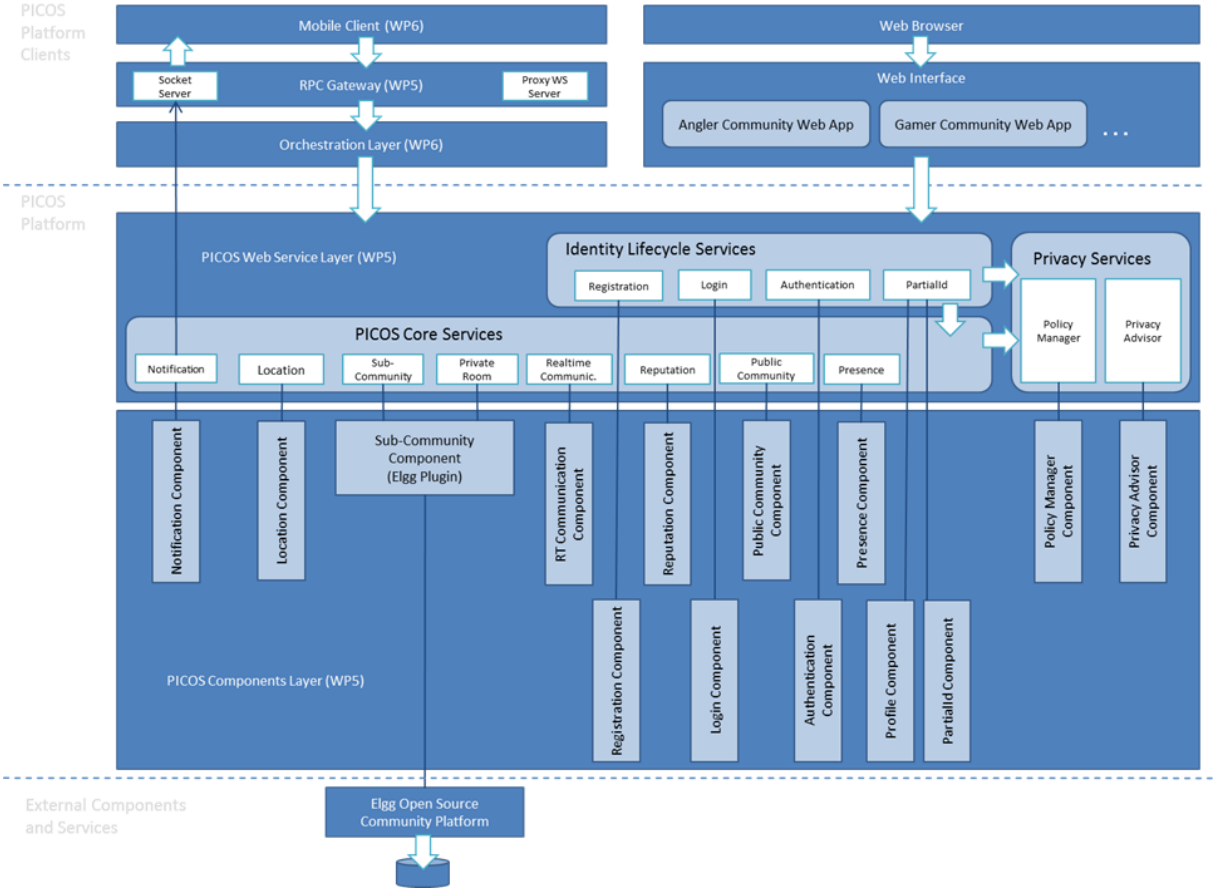


Figure 29 Infrastructure context – Client / Server / Service Provider

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

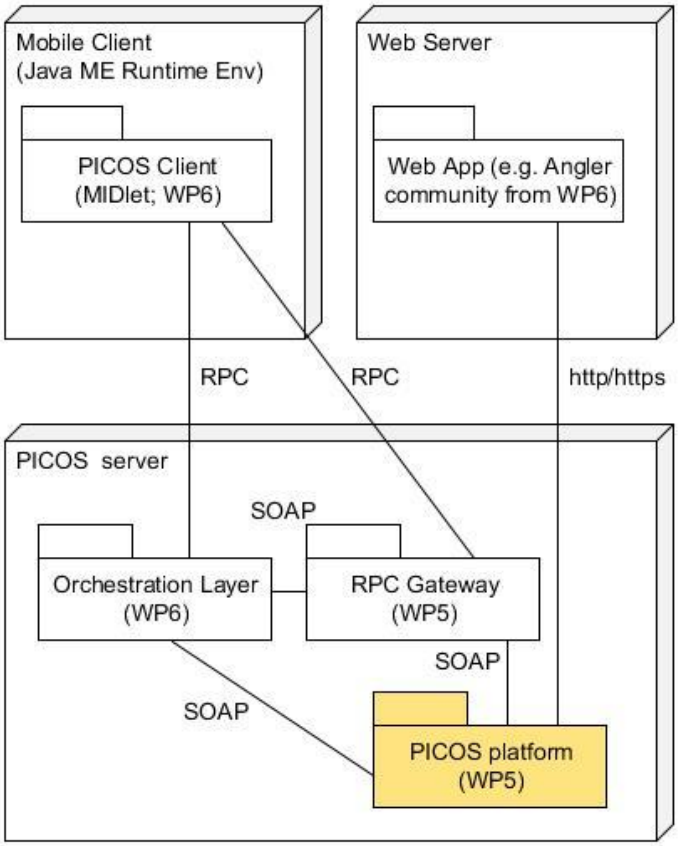


Figure 30 Infrastructure context – Service interaction

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

8.4 Privacy, Trust & Identity Management View

The architecture contributes to P/T/IdM through several key concepts:

- Partial IDs – Supporting *anonymisation*
- Privacy Advisor – Supporting *openness*
- Location Blurring – Supporting *anonymisation* at the context level
- Privacy Rooms – Supporting *confidentiality*

The components that implement these concepts are:

- Policy Manager
- Privacy Advisor
- Sub-community Manager

8.4.1 First Platform Prototype (WP5) contribution to trust principles

TrP1 Openness and Transparency

PICOS offers services that handle personal information in an open and transparent way. The WP5 PICOS platform implements the community policies that define how personal data is stored and made available. By default, all users' related data is private and cannot be accessed by any member of the community unless the user decides to make them public. The client application allows the customization of the privacy rules to enable partial sharing of data. Any modification of the privacy rules is logged for audit. All data entered by the End user is made available for modifications and the platform allows the modification of user-profile, published content as well as published contribution.

TrP2 Trust between communities

PICOS recognises trust as a common currency when exchanged between PICOS communities. PICOS trust relies on the reputation management which is designed to increase trust on members of the public community as well as trust of sub-communities. The sub-community member privileges are defined via policy rules and enforced by the WP5 components.

TrP3 Provenance

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

TrP4 External services

PICOS ensures that externally hosted services are delivered in a trustworthy way and that members are aware when external services are less trustworthy than internal services. External services have not been integrated to the PICOS framework implying no interactions between the WP5 PICOS platform and external unsecured servers.

TrP5 Audit

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

PICOS allows processes to be fully auditable by a trusted entity. The auditing relies on an Event logging component that collects logging from all components and allows a filtering of the event on a per user level.

TrP6 Objective/subjective trust

PICOS supports both objective and subjective methods for assessing trust. Trust relies on reputation and reputation is based on rating of content and contribution pushed to community or sub-community repositories. The reputation component is designed to filter reputation (and then trust) attacks. The reputation component offers a way to retrieve all rating events attached to content so that the history can be analyzed.

TrP7 Consensus

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.

TrP8 Member accountability

PICOS ensures that Members are accountable for their actions while a member of the Community. The event logging mechanisms, as well as the access control (validate user identity), 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.

8.4.2 First Platform Prototype (WP5) contribution to Privacy Principles

PrP1 Notice of collection

Notice is provided to the Data Subject of the purpose for collecting personal information and the type of data collected. The community terms and conditions explain the global community policies related to data collection and data retention. They are displayed before the final step in the registration process, just before the first screen on which data collection takes place.

PrP2 Policy Notification

Data Subject is notified of the applicable policies in terms of Consent, Access and Disclosure. The community terms and conditions explain the global community policies related to data collection and data retention. They are displayed before the final step in the registration process, just before the first screen on which data collection takes place.

PrP3 Changes in Policy or Data Use

Notice must be provided if and when any changes are made to the applicable privacy policies or in the event that the information collected is used for any reason other than the originally stated purpose. The WP5 PICOS platform is designed to respect user privacy and will enforce any customization of the privacy rules attached to user attributes. No data mining function is integrated into the platform and no external server is allowed to access the user data.

PrP4 Timing of Notification

The purposes for which personal data are collected should be specified not later than at the time of data collection. The community terms and conditions explain the global community policies related to

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

data collection and data retention. They are displayed before the final registration of a user as the first screen before any data collection. The terms and conditions must be agreed before moving to the data collection phase.

PrP5 Sensitive Information

Data Subjects must be informed of, and explicitly consent to, the collection, use and disclosure of sensitive information (i.e. information revealing medical or health conditions, racial or ethnic origins, political views, religious or philosophical beliefs, trade union membership or information regarding sex life) unless a law or regulation specifically requires otherwise. The platform offers way to share personal information should the user accept that sharing model. The user can change privacy rules and can request permission (for presence and location) to be asked for any accept to user data.

PrP6 Informed Consent

The Data Subject must provide informed consent to the collection of personal information unless a law or regulation specifically requires otherwise. The platform allows the user to manage consent via the policy rules that can be modified via the client application. Policy rule modifications are logged using the event logging.

PrP7 Change of Use Consent

Consent must be acquired from the Data Subject to use personal information for purposes other than those originally stated at time of collection. The platform strictly enforces default community policies (every user attribute is private) or the version customized by the end user himself.

PrP8 Consequences of Consent Denial

Data Subjects must be made aware of the consequences of denying consent. Any request denial to access user or platform resource leads to an error message sent back to the requester.

PrP9 Limitation of Collection

Only personal information relevant to the identified purpose may be collected. The platform allows the data collection of full user-profile attributes but restricts the mandatory entries to the very minimum (pseudo).

PrP10 Fair and Lawful Means

Information must be collected by fair and lawful means. Data collected by the platform are completely under the End User control. Some information is made public, which is the pseudonym or the partial identities, otherwise the default community policies block access to the End User information. Then the End-user can decide to allow access by other members to their profile, presence, location or contact list. Information is collected either during registration, partial identity creation or user profile modification using screen. None of the handset information is sent to the platform except the location information after the End User has enabled this capability and enable others to see his location information by customizing the privacy rules.

PrP11 Acceptable Uses

Personal Data may only be used for the purposes stated at the time of collection. User can create profiles that they can decide to share. Data are then collected for remote storage and it is up to the user to decide what to do with the data (push content and share it, share user profile , presence or location.

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

PrP12 Data Retention

Personal Data is retained no longer than necessary to complete the stated purpose. When the user is revoked, all user attributes are deleted. The event logging is kept for auditing purpose. No user data is kept in the event logging files.

PrP13 Third-Party Disclosure

Notice and Consent of the Data Subject is required to disclose information to third parties. The PICOS architecture must uphold the member's wishes with regard to information flow. No user data is disclosed outside the community and within the community, the disclosure is managed by the End User via the privacy rules.

PrP14 Third Party Policy Requirements

Organizations must ensure that any third parties are informed of their privacy policies and will follow them or possess equivalent policies. No external service is supported.

PrP15 Access to Information

Data Subjects are able to determine if an organization maintains data on them and should be able to request access to said information. Any data collected on the End User (user-profile, presence, location, contact-list, content in private room, forum contributions) is made available to the End User through the client application.

PrP16 Provision of Data

Requested information is provided clearly, at reasonable cost and within a reasonable timeframe. User Data are accessible when the user logs in and can be modified at any time during the session.

PrP17 Correcting Information

Data Subjects are able to update or correct personal information held by the community operator. User Data are accessible when the user logs in and can be modified at any time during the session.

Editor Note: PrP18 is intentionally absent from this list. It was considered unsuitable and abandoned, but we decided not to renumber the following privacy principles.

PrP19 Data Accuracy

Organizations will ensure that all personal information is accurate, complete and kept up-to-date. User Data accuracy is not managed by the platform.

PrP20 Public Policies

An Organization must ensure that its privacy policies are clearly published and publicly available. The terms and conditions contain the PICOS community policies. It is up to the client to enable the display of the terms and conditions at any time during the log-in session.

PrP21 Data Management

PICOS must allow members to express how to store and process their data and uphold their wishes in this regard. Not Applicable.

PrP22 End-to-End Privacy

PICOS supports end-to-end privacy. Not Applicable.

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

PrP23 Authentication

PICOS supports multiple forms of Member authentication, while continuing to respect privacy. The first prototype supports one way of authenticating the End user

PrP24 Multiple Persona

PICOS allows members to have multiple personas. See previous chapter to see how Partial IDs are managed with the platform. The multiple identities are not perceived by the WP5 PICOS platform as completely separated entities.

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

9 Research

9.1 Research overview

Research is an important element of the PICOS project, as demonstrated by the activities of the various Work Packages. In WP4, and in D4.1 and D4.2 specifically, we identified where we believed further technology research was necessary (e.g. where a feature was not well understood or had the potential to make a significant contribution to PICOS if developed beyond its current implementation). We marked these using the icon:

PICOS research

Eight components were identified as requiring further exploration:

- Accountability
- Data Minimisation
- External Recommendation
- Linkability
- Partial Identity Management
- Policy Management
- Privacy Advisor
- Reputation Management
- Trust Negotiation

We also identified new challenges:

- A stronger trust model
- Independent identity endorsement
- Independent law enforcement
- Move sensitive functionality to the client
- Privacy from Community Operator
- Location Based Services
- Points of Interests (POIs)
- Private Sites
- Search nearby gamers/contacts
- Advertising services

Much of this research is recognised in the components that have been specified and subsequently developed. In this deliverable we describe two further research activities that have a direct bearing on

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

the architecture and its components. Other research activities are reported independently as part of the PICOS outreach and dissemination programme.

9.2 Update on architectural Features and Components research

9.2.1 Advanced Targeted Advertising

9.2.1.1 Overview

The approach to targeted marketing for social networks (see 7.8.2) is based on current research at PICOS partner Johann Wolfgang Goethe-Universität, Frankfurt. The background to this research was initially outlined in [Kahl, Albers, 2010]. Meanwhile the approach was further elaborated.

The underlying concept originates from the idea that communication can be regarded as one of the main activities that takes place in social networks [Caroll, 2007]. Hence, in order to support marketing activities into social networks, marketing needs to be integrated into the context of these communication processes [Palmer, Koenig-Lewis, 2009]. Based on this approach, called 'marketing enriched user communication' [Kahl, Albers, 2010], marketing can contribute to the communication in two ways: First, marketers can provide targeted communication (personalised marketing, e.g. targeted advertisements) to social network users. Second, marketers can support the communication between users (viral marketing, e.g. via brand related groups) (Figure 31).

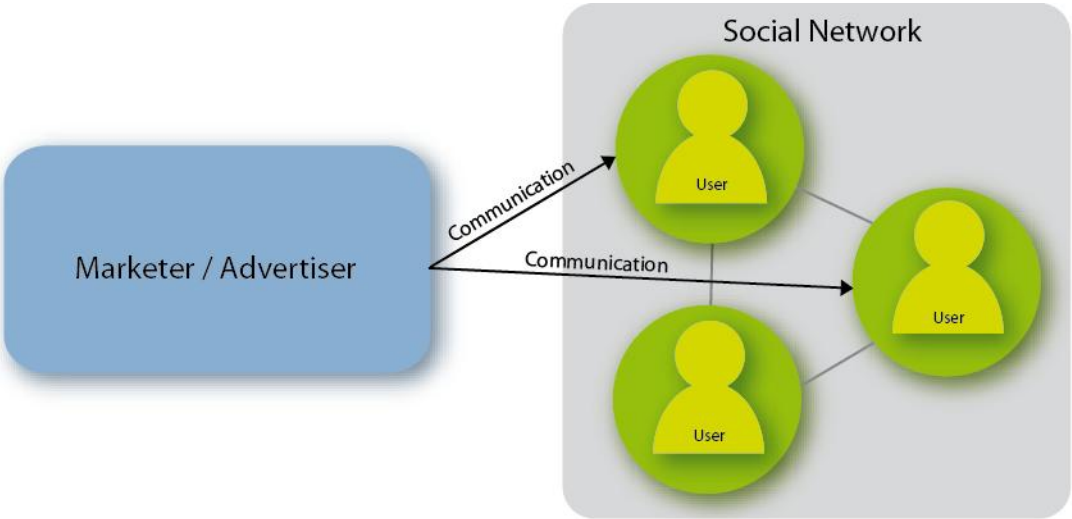


Figure 31 Communication relationships in Social Networks

Marketing must support both approaches while complementing existing forms of communication within communities, if it is to receive the attention of the participating users. While the targeting of marketing activities provides a benefit to the targeted users [Nielsen, 2009] [Ho, Kwok, 2002], at the same time viral marketing is used in existing social networks (see e.g. [Facebook]) to benefit from the intensive social interactions between users. By supporting both, the communication between

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

marketers and users is more tailored to the individual user, and consequently likely to be more relevant.

A complementary effect is that users are encouraged to communicate with each other about advertised content. If the content is perceived as relevant and useful information, users might recommend the content to other users who have similar interests [Schulz et al, 2007] [Dobele et al, 2005].

9.2.1.2 PICOS focus

The previously described general approach outlined how marketing could support the communication processes within social communities, and how it could thereby be integrated into these communities.

Our research focus is limited to *advertising* as one aspect of marketing. Other marketing aspects such as the *pricing* of products (e.g. pay per click, pay per view) are not considered. It should also be appreciated that advertising as a marketing activity that in practice is part of a social networks' business model, which usually also includes other aspects, e.g. the offered product or service itself. Advertising represents one aspect of a possible business model of a social network provider, to generate revenues.

9.2.1.3 General Approach

In communities there are two ways for how an advertising message can be communicated. First, the message can be communicated between a 3rd party (the marketer/advertiser) and the user. Second, the message can be communicated between a user and other users. From the business perspective these communication relationships can be referred to as Business-to-Consumer communication (B2C) or Consumer-to-Consumer communication (C2C). As previously mentioned, both kinds of communication are part of the concept of a marketing enriched user communication and hence both need to be supported by the PICOS Advertising component, following this approach (Figure 32).

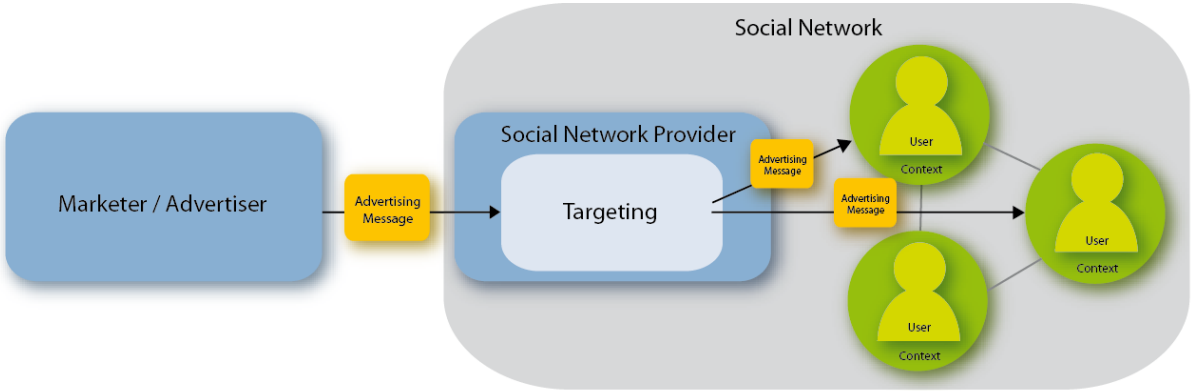


Figure 32 The Social Network Provider as an intermediary between Advertiser and User

In both cases the social network provider needs to provide a degree of transparency to the users, with regard to the use of their data. The provider should outline how users' data is used to support advertisements and the benefits of such an offering.

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

9.2.1.4 Support of B2C communication

B2C communication concentrates on communication between advertiser (3rd party) and user. The idea is that the social network provider acts as an intermediary between these two parties. From the PICOS point of view, this ensures that personal data is neither given to 3rd parties nor that 3rd parties have direct access to it. Instead, the social network provider (e.g. a Game developer in the case of the Gaming Community example) serves both the advertisers and the consumers, while respecting their specific interests (e.g. privacy of users). In particular the PICOS platform needs to provide on one hand an interface for advertisers, which allows them to configure what they want to advertise and to whom. On the other hand the provider needs to identify the users for which a particular advertisement might be relevant and provides them with this advertisement.

This trusted intermediary role that the operator has with regard to advertising is in keeping with the trust model that PICOS has adopted.

The social network provider thereby performs a matching process between the users (consumers) and advertisers (represented by advertisements), similar to an intermediary on a virtual marketplace who mediates between suppliers and demanders [Kollmann, 2006]. For example, a gaming community provider might identify a matching between certain users with an interest for strategic multiplayer-games and an advertisement for such a game.

In order to perform the matching process, detailed personal information (e.g. profile attributes) is needed. Using such personal information enables a precise characterisation of the user to be constructed. Social Communities already contain detailed personal data about their users, which can be further extended by including context information within mobile environments (e.g. location, date, time and device) [Schmidt et al, 1998]. Such additional information not only allows a more precise characterisation of users, but allows advertisers to draw conclusions (interpolate, extrapolate) about what users are doing. For example, in an angling community the actual location information of particular anglers could be compared to information about watercourses locations, in order to identify if an angler is currently angling at a watercourse. In addition, as previously mentioned, communication information (i.e. instant messaging) can be examined, e.g. for key words that fit to certain advertisements.

Targeted advertisements of this nature are supported by recent studies, which in general show a relationship between the degree of advertisements personalisation and gaining attention of users. More targeted advertisements receive more user attention, in particular, with regard to mobile usage scenarios [Ho, 2009] [Beals, 2010] [OFT, 2010]. These studies indicate that users are interested in targeted advertisements since they provide them with a certain level benefit, assuming that these advertisements relate to relevant and valuable content.

Against this background it is important for the social network provider to achieve a balance between the needs of the consumers and the interests of the advertisers, as well as the operator's own interests. The provider needs to consider the privacy preferences of his users during all possible activities including the relevance and usefulness of advertisements. At the same time the operator is expected to fulfilling the advertisers' goals of reaching a high percentage of closely matched users. Not least, the operator needs to ensure that his underlying business model, and in particular his revenues/profits are maintained.

The whole process of supporting B2C communication can be divided into four steps, which are reflected in the design of the PICOS Advertising component as follows (Figure 33 – which is based on [Kahl, Albers, 2010]).

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

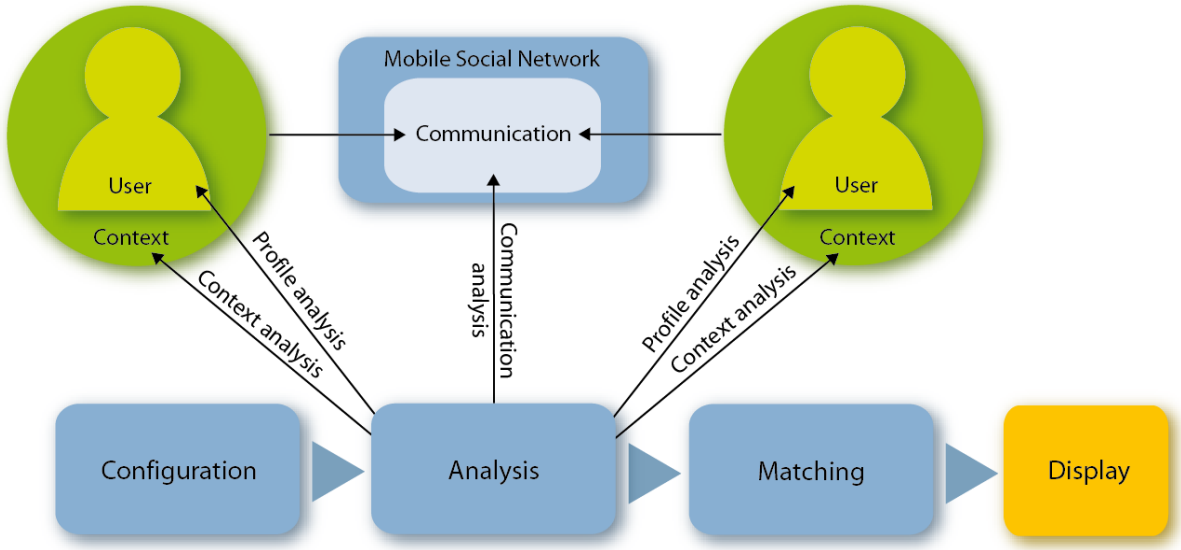


Figure 33 The process to support targeted advertising (B2C)

Step 1: Configuration (Social Network Interface)

The advertising component provides a graphical interface, which permit configuring of different advertising activities in line with member 'user-centric' wishes. As similarly described in [Albers, Kahl, 2008] [Verlag] [Hristova, O'Hare, 2005] [Kurkovsky, Harihar, 2006] the advertiser can configure what message he wants to deliver and whom he wants to target (cf. [Facebook]). Hence, the dimensions the advertiser needs to configure are the advertisement itself and the target profile.

The form of an advertisement can be a selection of different types, e.g. banners, pop-up, message, invitations to brand specific groups, such as the following: Advertising: 'Pop-Up' with Message: "Special Lunch offering! Only today between 1 PM and 2:30 PM at Pizza Joe."

By defining the attributes of the target profile, the advertiser can describe those users that he wants to target. This could potentially comprise all attributes that a user describes in his profile. In the example below, attributes like gender, age and the distance to the advertiser's shop are defined. The more precise this definition is, the more accurate is the targeting of individual users. A typical example might be: Target Profile: "male, 20-35 years, within 2 km around my shop, between 12 h and 18 h, key word in communication: 'lunch'"

In addition, the advertiser can configure how many attributes are necessary to provide a 'good match' between target profile and user profile. For each attribute the advertiser can also choose if matching an attribute is mandatory, e.g. a user needs to be at least 18 years of age in order to receive an advertisement.

Step 2: Analysis

In order to determine which advertisement might be relevant for particular users, information about the user is required. The requested information is gathered from the user profile, the user's context and communications/interactions with other users [Kahl, Albers, 2010].

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

The user profile in PICOS includes numerous attributes, e.g. age, gender, interests, and favourite locations, etc. The context information is mainly describes the current location of the user (as geo-coordinates) linked to time and other information that might be derived from the location (e.g. current weather at this location). Communications could be any interaction in which a user shares information with other users, e.g. directly, by mailing or chatting as well as indirectly via comments or contributions in sub-communities. The gathered information leads to a dynamic user profile, which contains the profile, the context and communication information about the user.

Step 3: Matching

The dynamic user profile characterises the user in his current context. It thereby represents the complement to the target profile, as defined by the advertiser, which characterises the targeted user for an advertisement. In the so-called "matching" process the dynamic user profile and the target profiles are compared.

There are different ways how to realise such matching in an actual implementation, and the chosen way, might depend on various economic, organisational or technical factors. For example, with the PICOS gaming community prototype, a comparison of attributes is performed, and if a pre-defined number of attributes match, a matching is recorded (see Step 1: Configuration).

Example:

1. Dynamic User Profile: "female, 28 years, 1.5 km away from shop"
2. Target Profile: "female, 20-35 years, within 2 km around my shop, between 12 and 18 h
3. Keyword in communication: 'lunch'"

All 3 attributes of the dynamic profile are matching with the target profile.

In the approach described by [Kahl, Albers, 2010], the matching additionally contains a comparison between the communicating users. This is to identify similarities and common interests between them, and to present matching advertisements not one but both user identities.

Step 4: Display

In the final step of the process, the actual advertisement needs to be shown to the previously identified matching users. In practice this would also include further considerations regarding the users' device. It might be necessary to adapt the advertisement, due to technical specifications or limitations of particular devices and/or operating environments.

9.2.1.5 Support of C2C communication

The support of user-to-user communication (or consumer-to-consumer – C2C) is the 2nd step in the integration of marketing into social networks, and complements the direct communication between advertiser and user (B2C). Based on the principle of viral marketing (cf. [Kotler, Arnstrong, 2006]) the marketing message is spread from one user to another users (and so on) just like a virus. The goal of the advertiser is to establish and gain support for a viral (marketing) process. This process is part of the communication between users and, as such, it complements the direct communication between Business and Consumer.

In literature and practice there is a varying understanding about how viral marketing works in detail [Phelps et al, 2004]. In many communities viral marketing is conducted by introducing a product or brand to the community (e.g. with a related profile or group on Facebook or MySpace). In these cases,

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

basic principles of social networks are applied to commercial products, namely to present oneself (the product) and communicate with others (customers). Unfortunately, such a communication is unlikely to influence or direct customers, and is not considered to be a targeted approach. In our case, viral marketing is designed to work in a more targeted way so as to select the hopefully more influential users (a.k.a. 'opinion leaders'), who further spread the message [Dobele et al, 2007].

As considered in PICOS, this process can be described as comprising the following steps (Figure 34):

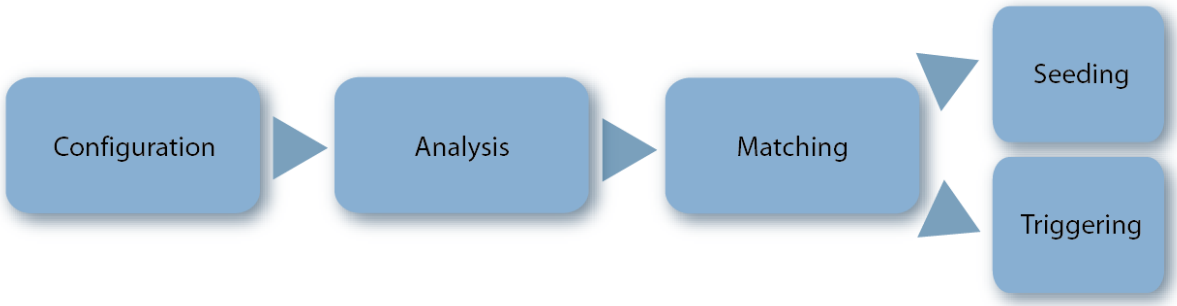


Figure 34 The process to support Viral Marketing (C2C)

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

Step 1: Configuration

The first step represents the configuration of the Marketing Message (Advertisement). Basically, the activity is similar to the configuration in B2C support (as described previously): The advertiser has various options to configure an advertisement and to describe the targeted user for this advertisement. This includes the specification of the target characteristics (e.g. Age, Interests). The configuration includes as well options regarding the form of the delivery (e.g. pop-up, text message, etc.).

The difference is that the advertiser in this case defines the characteristics of the "key users", which should be addressed in order to further spread the advertisement. These users are regarded as opinion leaders, who have a stronger influence on their social surrounding [Dobele et al, 2005] [Phelps et al, 2004]. Depending on the actual advertisement to be delivered, there might be different definitions of who the 'key users' are. In general, it might be users who are very active with regard to communication. In other cases it might be users who have many relationships to other users (friends) or who have certain characteristics (e.g. a certain age). The definition of key users might also be a combination of such different characteristics, such as a number of the most active users who live in a certain geographical region. The configuration interface needs to support the consideration of such aspects wherefore further, more general data about users might be required (e.g. number of friends, activity based on e.g. number of community contributions).

Step 2: Analysis & Matching

While the target profile configuration is different, the Analysis and Matching process itself is similar to the respective steps for targeted advertising (see the sub-section on Support of B2C Communication). The analysis contains the analysis of user information (profile, context, communication) which leads to a dynamic user profile, as described previously. In the 'matching' step, the characteristics of the key users (target profile) are compared to the dynamic profile of a user. The difference to the Matching process for targeted advertising is, that only a limited number of matching users are addressed, namely the key users. These users are the users which match best with the target profile.

Step 3: Seeding

This phase includes the actual delivery of the marketing message to the identified key users (see step 2), the so-called "seeding", in order to allow them to pass on the delivered message. Depending on how an advertisement is configured the form of delivery may vary. In order to ease the forwarding of the delivered message, advertisements should contain a possibility to immediately share them with other users (e.g. context Link on a specific site, Banner with possibility to forward, etc.).

Step 4: Triggering

The whole viral marketing process is intended to support the viral distribution of the advertisement. Hence, an important part in this approach is not only to identify adequate users and provide them with the advertising message, but also to provide or support a motivation to these users to forward the advertisements they receive [Pousttchi et al].

One step that supports this is the targeting itself, considering that we aim to provide only highly relevant advertisements to users. Furthermore, an existing intrinsic motivation of users to forward advertised messages can further be supported by the availability of technical possibilities, which allow and simplify a further recommendation to other users. In the PICOS Gaming Community Application prototype such a support will be e.g. realised by providing a forward button in the advertisements for the so-called 'commercial Points of Interest'.

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

9.2.1.6 Component Structure

The PICOS Advertising component supports two types of marketing activities for mobile social communities, as described in the approach above: support of direct targeted advertising between an advertiser and a community user; targeted ignition of viral marketing.

The goal is that both activities complement on another. Thereby, the component is intended as an exemplary showing how advertising can be integrated into a mobile social network context.

The component comprises two parts: One for targeted advertising and one for viral marketing. Both support the respective marketing process and therefore depict the structure of this process.

The triggering step is not specifically a part of the Advertising component – it is part of various different elements of a social community – and is therefore not described further. For example, the mechanism of 'recommendations' used in PICOS to trigger users to forward advertised *points of interest* (POI) can be implemented as a part of the respective component, which do not necessarily need to be the advertising component. In general, the concept of triggering is part of the components they affect, e.g. recommendations.

Targeted Advertising

The targeted advertising sub-component contains the following four elements:

Configuration Interface: This user interface provides a configuration in order to allow an advertiser to configure targeted advertising activities. The advertiser can specify the characteristics of the targeted users, based on available profile attributes (e.g. gender: male, age: 20-35 years, interests: gaming) including characteristics of the targeted context (e.g. time: 12-18 h, location: within 2 km around my shop) and usage situation (Communication). How detailed such a target profile should be, can thereby be decided by the actual advertiser.

The advertiser is further able to configure the advertised message. This should at least contain the message itself and the option to specify its form. Possible forms could be e.g. pop-ups, message or similar. Further forms may depend on the used underlying technology (e.g. Smartphone operating systems could allow more sophisticated advertisements, such as "Apple iAds").

Analysis Module: This module gathers information from the users' profile, their context and possible communications/interactions with other users. This leads to a dynamic profile, including all the gathered information. Before the gathering is conducted, the Analysis module checks the privacy preferences of the analyzed user and considers the attributes in accordance with these preferences.

Matching Module: For the matching process, the data of the previously created dynamic user profile is used. The matching module performs a comparison of each attribute of the dynamic profile with the attributes of the target profile. If the number of attributes s reached which need to be equal between both profiles, a matching is given.

Display Module: If a matching is given, the Display Module shows the advertisement to the user, according to the form specified by the advertiser. The module is responsible for an adequate display of the advertisement on the users' device.

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

Viral Marketing

Editor Note: See earlier Editor Note in sub-section 7.8.1 on the challenges that PICOS is encountering as it balances the needs of viral marketing and the PICOS principles on trust and privacy.

Configuration Module: The configuration is similar to the configuration of *Targeted Advertising*. The advertiser configures the target profile of the key users and the form of an advertisement (as described previously).

Analysis Module: Works in the same way as for targeted advertising. In addition meta information about a user, required for the matching process is analyzed (e.g. number of users).

Matching Module: The matching performs a comparison between the target profile of the key users and the respective dynamic user profile. Besides the profile comparison, further the previously gathered meta information is considered. Only the specified number of key users is finally addressed.

Seeding Module: The seeding module performs the actual delivery of the advertising message to the identified key users. The module shows the advertisement to the key users, according to the form specified by the advertiser. In addition, in order to trigger users to pass on the delivered message, a forwarding/sharing mechanism is integrated for all types of advertisements. This could e.g. be a button in a pop-up message, which allows selecting other users to share the message with (Figure 35).

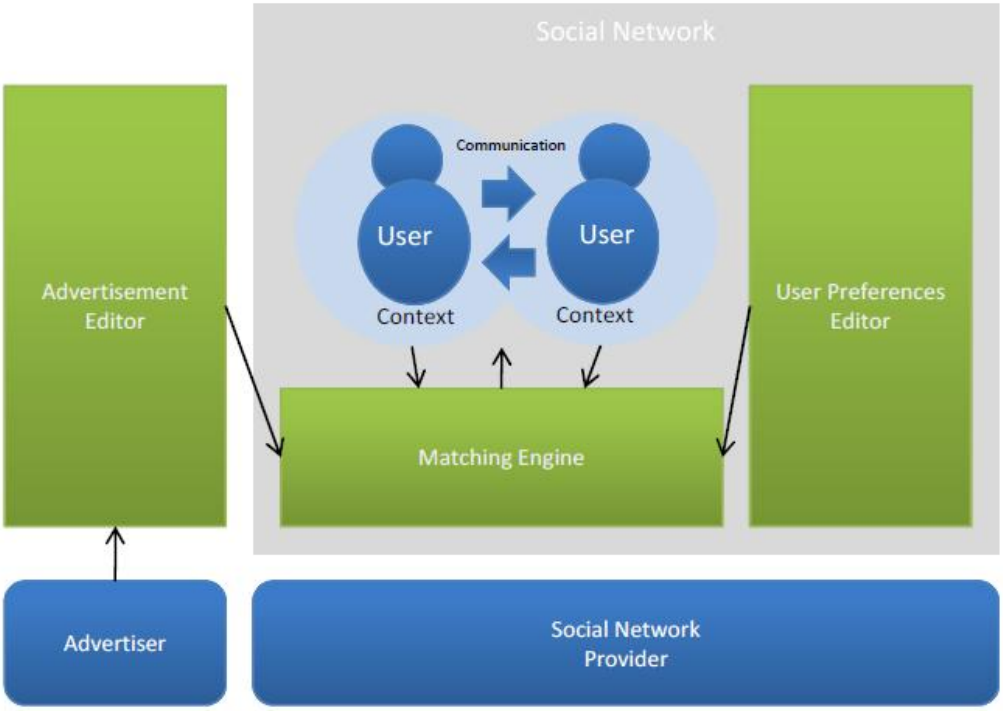


Figure 35 Structure of advertising component

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

9.2.2 Privacy Advisor

The Privacy Advisor (PA) is a distinguishing feature of the PICOS architecture. Its role in the first prototype was restricted to three functions:

- Content Awareness (scanning)
- Sub-community Dynamics Awareness (reputation)
- Workflow Awareness (revocation)

The full potential of the PA extends beyond these three functions, and includes:

- Enhanced Content Awareness
- Privacy Rule Matching
- Social Presence Awareness

The overriding intention is that the PA plays a role in a broad range of situations where a PA, acting as a member's 'best buddy', 1) helps build trust and 2) minimizes undesired exposure of personal information. The PA is invoked in situations where personal sensitive information is unintentionally revealed, or situations where trust is potentially misplaced, e.g. revealing a name alongside a picture or interacting with members who have a lower that expected reputation.

9.2.2.1 Enhanced content awareness

Role of the PA

Scanning is extended to include:

- personal information contained in the content of member contributions, when
    - shared with sub-group members, and
    - when shared publicly

Scanning concerns 1) content tags (e.g. name, description, etc.) and 2) the body of the content contributed (where the body is interpretable).

The examination involves the matching the above mentioned tags and body with 1) previously defined personal information stated in the member's profile, and 2) predictable information (e.g. email address, credit card number, telephone number).

The PA reports on the analysis of member profiles, and notify the member where the content is considered by the PA to be sensitive.

Since image sharing is an important feature of the PICOS, and anticipated to be used extensively by anglers, some level of image analysis should be included.

Operation

Two situations exist:

- A member is about to *intentionally* disclosed information that is personal and sensitive.
- A member is about to *accidentally* disclosed information about themselves, having previously stated that the information is personal or personal-sensitive.

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

In both cases, the PA detects and notifies the member so that they can consider if the disclosure is absolutely necessary.

9.2.2.2 Privacy Rule Matching

Role of the PA

The PA performs Privacy Rule Matching when as member joins a sub-community, where the PA will check the member's own privacy rules against the rules of the sub-community or the sub-community creator/owner, i.e. the sub-community inherits the privacy rules of the creator.

Operation

- The PA compares the privacy rules of the member who is joining the sub-community with the privacy rules of the sub-community
- The examination takes place in-between the requesting member making the request to join the sub-community and membership being accepted
- The examination involves the matching privacy rules

The PA retrieves and compares the two sets of privacy rules, field by field (using ID1/ID2 to locate the privacy rules for member and sub-community). An exception results in a notification being sent to the joining member. Exceptions are defined as 1) a difference in values (e.g. only interact with female members vs. a male member), or 2) an out-of-bounds variation (e.g. only interact with member of neutral or positive reputation vs. member with negative reputation). The PA is able to determine the correct type of comparison to use.

9.2.2.3 Social Presence Awareness

Role of the PA

The PA notifies the member if they publicly revealed their position in high-risk settings (locations), and suggests suitable remediation, i.e. turn of or blur/increase blurring.

Operation

Three examples are:

- A member is notified if another member, who is not a member of any of their sub-communities, attempts to access their location.
- By default, a member blurs their location. However, they may choose to turn blurring off, e.g. when beside a lake where they would like other anglers to visit to chat.
- The member moves to another location (e.g. home) but forgets to turn blurring off. The PA warns then that they are revealing too much information.

For the PA to operate successfully, it is necessary to pre-define 'locations', i.e. bounded geographical areas, e.g. at home, at work, by the lake.

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

9.2.3 Privacy-respecting Reputation Management

Research into how reputation information can be both privacy–respecting and at the same time contain sufficient provenance so that is considered trustworthy by community members and the community operator is still on-going.

9.3 Research outlook

The advertising approach presented in this document builds upon previous research with regard to context aware targeted advertising, which was enhanced and applied in the context of PICOS. The advertising approach will be subject to further research on a conceptual and practical level.

Focus of such further research will be on more advanced mechanisms to consider user related data (profile, context, communication), especially with regard to context and communication. One of the main questions will be which information context and communication can provide and how to use such information for targeting ads in a given situation. In order to answer such questions, the approach will need to be applied to more specific application domains, in order to outline exemplarily for these domains how the approach could be applied and how it can provide benefits.

In addition, besides the evaluation in the PICOS user trials further practical evaluation needs to be conducted in order to confirm the potential benefits of this approach. We expect the gamer trial to raise new dilemmas too.

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

Section 3 – Prototype enhancement thread

10 Introduction to Prototype enhancement thread

This section describes the architecture from the point of view of the second cycle prototype development activities that run in parallel to the second cycle architecture development.

The description follows a similar format at the architecture design and research thread, in that it describes the architecture (in this section, the prototype architecture) using the new model view approach, namely:

- Building block view
- Deployment view

We begin with a details explanation of the new requirements that arose from construction of the first prototype and associated user trials, and that which ultimately go to make up this PICOS Platform Architecture and Design 2 deliverable.

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

11 Implementation considerations

11.1 Requirements

Following the creation of the first cycle platform and application prototypes, and the subsequent trials, we undertook a process to identity what changes needed to be made to each prototype in order to support the second phase of angler trials and the upcoming gamer trial.

The new requirements had arisen from several sources:

- The users who took part in the trial
- PICOS partners who attended and supported the trial, and who observed the need for new, updated or improved features
- The whole of the PICOS team who wanted to see additional features tested in future trials, where this had not been possible in the first trial, due to time constraints imposed on the developers and trial designers
- The outcomes of the assurance work (Assurance requirements)
- Feedback from the EC reviewers at the 1st PICOS project review
- Deliverable D8.1

The process of analysing these was undertaken in two stages and captured in internal project documents R1 and R2. R1 identified new requirements and ranked them according to value to the end-user. R2 investigated the implications of meeting those requirements and ranked them according to value to the project of meeting them, this ranking taking into account the insights that would likely to be gained and the implementation time and resources required.

A detailed description of the R1/R2 requirements can be found in Appendix F.

11.1.1 Requirement-collection (Requirements gathering stage - R1)

The first stage, R1, involved listing all new requirements, and then ranking them as:

- Absolutely necessary (Category 1)
- Extremely useful (Category 2)
- Somewhat useful (Category 3)
- Nice to have (Category 4)

Note: Experience later showed that a better classification used three classifications: necessary; recommended; helpful. This approach was adopted when valuing the gamer requirements.

In addition, the categorisation process took into account:

- What the requirement aimed at addressing:
  - something that was not addressed in the first prototypes
  - aimed at improving something that was addressed in the first prototypes

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

- Would addressing the requirement have a:
  - localized and restricted impact on the second prototypes
  - wider impact thereon

A total of 23 requirements for the gamers and 37 requirements for the anglers were identified. This list covered:

- Multi-Communication
- Organisation of ad-hoc meeting
- Marketing/Advertising
- Real-time content sharing
- Enhanced Social Ads
- Virtual marketplace
- Marking a place (geo-location) as a Point of Interest (POI)

11.1.2 Investigation (Requirements gathering stage - R2)

The investigation resulted in the following choices of implementation value, i.e., the cost/feasibility of doing so versus the likely contribution to insight or understanding (technical or social science) of the PICOS main concerns (Trust, Privacy, Identity Management):

- Necessary:
  - Sharing Contact-List
  - Restrict access to published content
  - Restrict access based on date condition
  - Enhance Content Awareness
  - Social presence awareness Point of Interest
- Recommended:
  - Notification for new available content
  - Content access history (public community)
  - Public Point of Interest
  - Custom Point of Interest
  - Private or public Point of Interest
  - Advertising services
  - Revocation
- Helpful:

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

- REQ: Gamers Requirement R9: Shared desk (combined with Requirement R12)
- Real-time chat
- Reminder (notifications)
- Reminder (sharing)
- Enriched status information
- Meeting with nearby players
- Real time content sharing
- Archive chat
- Offline notifications

The following features were identified by the trials as useful for enhancing privacy and trust, and are to be developed for the second cycle user trials:

- Privacy
  - Sharing contact-list
  - New profile for Gamers
  - Privacy rules for content based on access restriction for contacts and time
  - Presence note available in the profile
  - Privacy Advisor extended to scan for additional personal information
  - Points of Interest. Definition of a POI
  - Private Sites. Automatic management of presence, including blurring close to a location
  - Locate nearby (online) gamers
  - Advertising service based on POIs, targeted by exposed profile attributes.
- Trust
  - Rating of Points of Interest
  - Sharing contact-list in which contact rating is also available

There was no enhancement requested that specifically addressed identity management.

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

12 Architectural description

12.1 Highlighted enhancements to Angler prototype

12.1.1 Mobile application

The mobile application part of the Anglers Prototype v2 is based on the R2 document. The following outline summarizes the area where changes in functionality were agreed:

- Registration, including profile completion
- Access to the Community
- Partial Id Manager
- Profile Manager and Policy Manager
- Policy Creator, including meta-objects reference

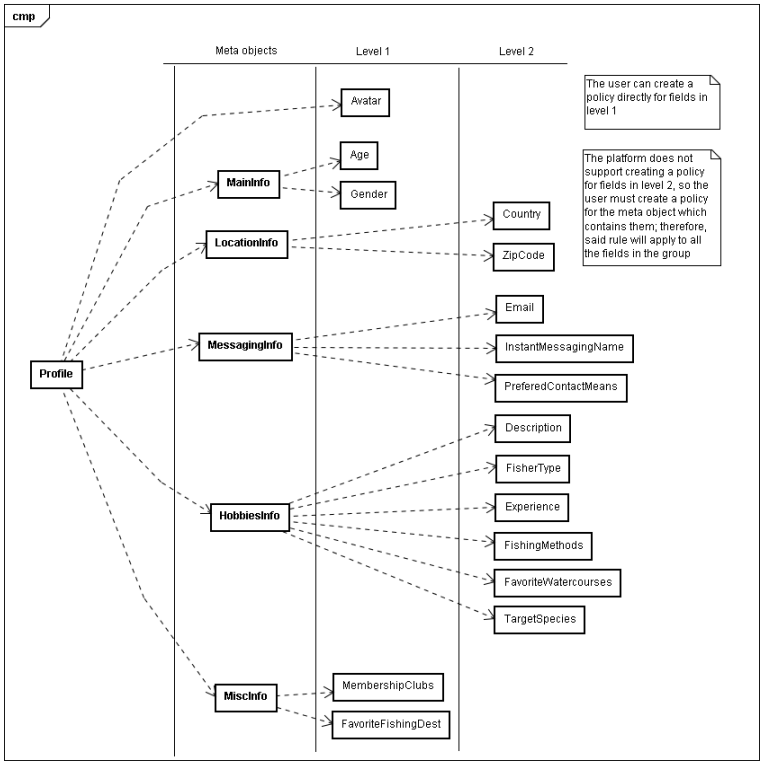


Figure 36 Meta-object reference diagram

- Contacts Management
- Privacy Advisor
- Public Community

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

    - Possibility to modify the content of a post when this has not been rated yet by other members of the community.
- Public repository
    - Category attributes edition: the category attributes can now be updated by the owner
- My Files: No major changes.
- Sub-Communities: No major changes.
- Species Summary: No major changes.
- Location based services (fishing spot/watercourse advisor)
    - Location Use cases
        - Show my location on map
        - Centre map on my location
        - Add/Edit Fishing Spot
        - Add/Edit Watercourse
    - Contact Location Use cases
        - Show location of contacts on map
        - Centre map on location of contact
        - Show contact address
    - Watercourse Location Use cases
        - List Watercourses
        - Reload Watercourses
        - Show Watercourse Details
        - Show Watercourses on Map
        - Centre Map on Watercourse
        - Delete Watercourse
    - Fishing Spot Use cases
        - Reload Fishing Spots
        - Show Fishing Spot Details
        - Show Fishing Spots on Map
        - Centre Map on Fishing Spot
        - Delete Fishing spot
- Real time content sharing
- Additional Improvements: GUI improvement, layout improvement, help buttons, usability improvement.

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

12.1.2 Web Front-end extension

A Web front-end (AnglersBase) was developed as a mirror of most functionalities of the mobile application (except those related to LBS): Partial IDs, Contacts, Public Community, Sub-communities and Private Room.

This is not a mobile component, but it enriches the global architecture by extending the functionality to a PC. This also proves the interoperability between mobile and PC environments.

12.2 Building block view

D5.1 and D5.2a implements several components in specific ways for the purpose of simplification, including:

- Scenario Management is part of the Privacy Advisor
- Intrusion Detection is part of network security and/or relates to Feedback and/or Misuse Reporting
- Importer/Exporter has been substituted by Private Room; a Preparation Area is not needed
- The Consent Manager was not realized by D5.1, but is still of relevance

12.2.1 Mapping components from WP4 architecture to WP5 platform

The architecture components the WP5 selected for inclusion in the first PICOS prototype are:

- Access Control
- Authorisation
- Partial Identity Manager
- Privacy Advisor
- Location Sensor
- Notification
- Registration
- Sub-community management (include private rooms and non real-time content sharing)
- Authentication
- Reputation Manager
- Service Selector
- Privilege Manager
- Profile Manager
- Privacy Manager
- Social Presence

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

- Real-time Content Sharing

D5.1 gave an overview of the different components that were implemented in the platform prototype, and pointed out that although the names of the architecture components and the names of the platform services are very similar, there is not necessarily a 1-to-1 mapping between each. In fact, in some cases the functionality of the architecture component is achieved by combining multiple platform components, where the application is responsible for invoking the platform components in the correct sequence.

D4.1 component	**WP5 interpretation**
Registration	Implemented as a combination of the WP5 Registration, Partial Id and Public Community components
Authentication	Implemented by the WP5 Login and Authentication components
Authorisation	Implemented within each WP5 component with support from the Policy component
Access Control	Implemented in the WP5 as the Proxy Web Service
Partial Identity Manager	Implemented in WP5 as the Partial Identity component
Privacy Advisor	Implemented in WP5 as the Privacy Advisor component
Location Sensor	Implemented in WP5 as the Location Component
Notification	Implemented in WP5 as the Notification component of the RPC gateway
Privilege Management	Implemented in WP5 as the Policy component
Profile Manager	Implemented in WP5 as the Profile component
Policy Manager	Implemented in WP5 as the Policy component
Reputation Manager	Implemented in WP5 as in the Reputation component
Sub-community and Asynchronous content sharing	Implemented in WP5 as the Sub-Community component

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

D4.1 component	WP5 interpretation
Service Selector	The component is NOT implemented by WP5. The assumption made by WP5 is members' access to services is under the control of the resource policies, and therefore enforced by the owner of the particular service.
Social Presence	Implemented in WP5 as the Presence component
Real-Time Content Sharing	Real-Time Content Sharing is derived in WP5 from the general content sharing functionality described in D4.1, but the focus is on real-time content sharing through establishment of communication channels between participating components

Table 10 WP5 interpretation of D4.1 component

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

Section 4 – Outreach

13 Standardisation

PICOS is active in standardization activities and has established a liaison with the ISO/IEC JTC1/SC27/WG5 Standardization Committee on Biometrics, Identity Management and Privacy.

The WG5 is currently working on approximately a dozen documents. For the merit of the work of the PICOS project the most relevant working item is the draft of the ISO/IEC 29101 titled 'Privacy reference architecture'. So far the PICOS project has contributed twice with its comments related to the draft of the ISO/IEC 29101. In November 2009 the PICOS contributed with 11 comments, of which the majority were accepted. These technical comments were aimed to clarify the text and to enhance a few paragraphs of the draft. In April 2010 one major contribution was submitted (it was assigned the identification number N8072). The comment/contribution included an example architecture for privacy enhanced community services. The example architecture is based on the PICOS architecture, i.e. on the work done within WP4. The example architecture for privacy enhanced community services derives from D4.1. It is high level and abstract allowing implementations in many different domains and environments. The PICOS architecture as described in D4.1 has been significantly simplified to fit better the purpose and style of the draft of the standard. Many elements were grouped together to form logical modules. On the high level of abstractness the move from D4.1 to D4.2 does not play an important role and the simplified architecture remains fully compatible with this deliverable D4.2.

13.1 PICOS contribution of ISO/IEC 29101

Before the April 2010 WG5 meeting the draft of ISO/IEC 29101 was in the 5th WD (working draft stage). During the meeting the PICOS comment/contribution with the example architecture for privacy enhanced community services was accepted and the example architecture was included in Annex A.3. The submitted text was slightly modified by the editor of the project (i.e. the draft of the standard) and it covers two and a half of pages. During the meeting of WG5 it was also decided to proceed with the draft of the 29101 Privacy reference architecture thus creating the first CD (Committee Draft stage). It is planned for the draft of 29101 be voted on for final International Standard in the fall 2011. The following sub-section includes the content of the Annex A.3 of the draft of ISO/IEC 29101 as it appears in the 1st CD of the standard.

13.2 Description of the example architecture

The example architecture described here is designed for maximum flexibility and is, therefore, essentially topology-agnostic. It is a service-orientated design with services targeting the community member in the first instance but supporting inter-member relationships and community management.

Achievement of privacy is dominated by the use of a concept called partial identities. Partial identities provide community members with the ability to operate anonymously while at the same time ensuring

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

that other community members and the community operator (which in a peer-to-peer configuration may simply be a collection of other members) are confident (have trust) in the integrity of others and can fulfil legislative requirements. Partial identities offer conditional anonymity but support law enforcement and a desire for enhanced trust and openness between members. The condition element of conditional anonymity is governed by a trusted authority which can be an external independent body, a trusted collection of members or an outsourced hosting entity.

Individuals mainly establish trust using the specially designed reputation mechanisms, although the openness and informative style of the architecture also help. These same mechanisms help the whole community understand any risks associated with sharing personal information and as such raise the level of trust throughout the community and between individuals. Privacy respecting reputation ensures that despite members being allowed to have multiple (partial) identities, they remain accountable through a single private overarching identity. The reputation management features of the architecture satisfy the subjective nature of reputation. They provide a reputation defining mechanisms but do not set thresholds for trustworthy member behaviour.

A privacy advisor further enhances member privacy by checking member activities in real-time, by (1) looking for evidence of activities that may undermine the member's attempt to remain private, and (2) by educating the member when the subtitles of a member's actions may expose sensitive personal information. The privacy advisor acts solely on behalf of and is loyal to a community member, except where member actions are not in the best interest of the community as a whole, or where the action may be illegal within the jurisdiction(s) where the community operates. In this respect, the privacy advisor is truly personal.

Members preserve privacy by interacting with one another in private 'rooms' (they can also interact in a more ad-hoc public manner but must acknowledge some loss of privacy). Private rooms allow members to share content in a controlled way, restricting readership with regard to the reputation and privacy concerns of targeted members. Content can be anything from simple messages through to multi-media attachments. The potential for the member to accidentally reveal private information about themselves during this type of exchange is minimised by the use of the privacy advisor.

The architecture considers the full lifecycle of membership activity, from registration with the community, interaction with other members, use of shared facilities, and ultimately concerns that arise when a member terminates membership of a community but leaves personal artefacts behind.

The example architecture was built upon a set of principles which in turn defined features that are derived form typical requirements for community services including mobile communities. Features are translated into system components that operate at varying levels of abstraction, and which together form a simple component hierarchy. The components can be grouped into modules covering the functionality of the community services in 10 modules: registration, multiple (partial) identities, access management, privacy advisor, social presence, reputation, revocation, external services, sub-communities and content sharing.

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

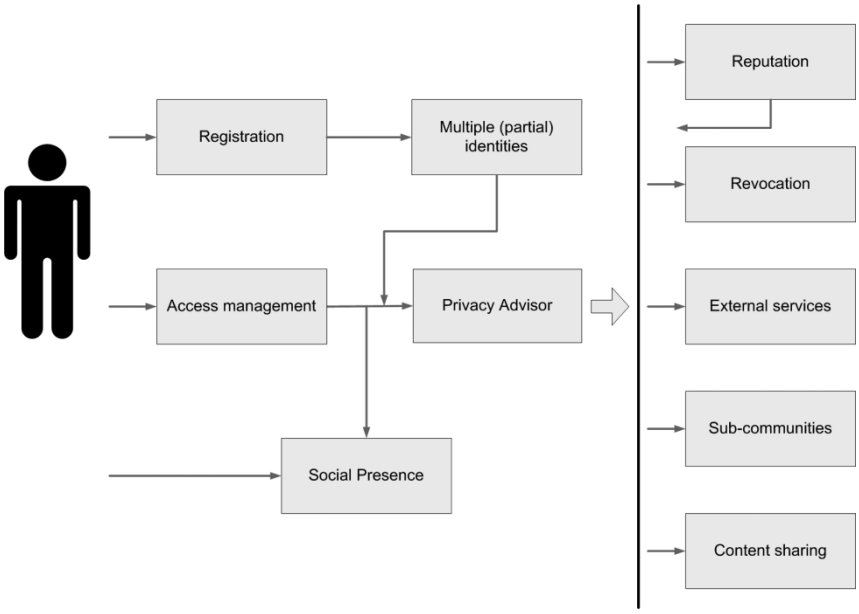


Figure 37 The example architecture for privacy enhanced community services.

The overall architecture is shown in the Figure 37 with the following elements:

- The privacy advisor module is based on the service selection component and receives also input from the consent management and reputation management components.
- The registration module receives input from the user and is interacting with the policy management, profile management and consent management components.
- The multiple (partial) identities module consists of the partial identity management and anonymisation components and closely interacts with the profile management, reputation management and event logging components.
- The access management module covers the authentication and authorisation components and cooperates with the profile management, social presence, consent management and event logging components.
- The reputation module is based on reputation management, feedback management and partial identity management components and it interacts with the personal profile management and event logging components.
- The revocation module consists of the revocation, policy management and personal profile management components. The module also notifies the event logging, reputation management and content sharing components.
- The external services module uses the partial identity management and external service delivery components to provide for external services. Events are logged via the event logging component.

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

- The sub-communities module is based on the profile management, sub-community management, delegation and consent management components. Events are logged via the event logging component.
- The content sharing module is built on the import/export, secure repository and content sharing components with the help of notification, event logging and personal profile management components.

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

14 Working with existing communities and technology

Although D4.2 is not primarily concerned with implementation as an add-on to legacy real-world community systems, issues of building a practical architecture have arisen in discussions between PICOS partners. The focus of the discussion has been on platforms, architectures and applications. Two interpretations have emerged that provide a useful insight into how PICOS might be built. However, the final decision on how best to construct the prototype remains with WP5 and WP6.

In sub-section 8.3.1 we discussed topologies, mainly client-server and P2P. Even so, it is not at first obvious where the optimal split in functionality between client and service lies. Therefore, options to distribute functionality across platforms on the client, server or both sides need to be considered.

It should also be noted that beyond the prototypes and the project, to achieve widespread deployment PICOS will almost certainly have to integrate with existing community platform technology, whether community management platforms, identity management systems or platforms that offer mobility support. This introduces an extra level of complexity, since PICOS cannot simply assume that the community application runs on top of the PICOS platform. Rather, PICOS needs to consider the case where the community application uses other (existing) middleware and services, e.g., services for community management, content sharing, for identity management, etc. This added complexity means that PICOS must offer extensions to existing middleware/services, rather than being a set of independent services. This third possibility is illustrated in the final diagram in this sub-section (Figure 41). For example, an operational community will have communication and content sharing facilities already, and will look to PICOS to provide the additional privacy enhancing features. This is one reason why a PICOS Toolbox approach makes sense when dealing with legacy systems.

As mentioned earlier, PICOS will need to inter-operate with established communities and existing technologies. One approach to achieve this is as follows (Figure 38):

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

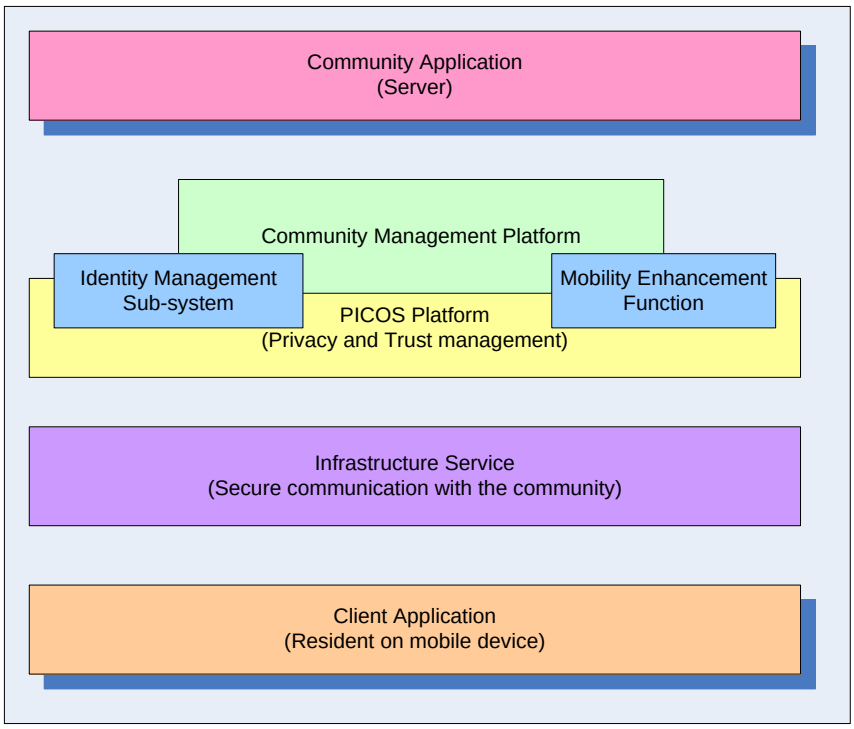


Figure 38 Implementation regarding existing communities

For mobile communities, or communities that want to offer services to mobile users, the same set of extensions can be applied to the community mobility platform (shown as the 'mobility enhancement function' in the above diagram). Some functions of the PICOS platform may actually be implemented as extensions to this mobility enhancement function.

With a main focus on privacy and trust management, the PICOS platform will rely on the underlying infrastructure to provide generic security features, for example for secure connectivity between mobile devices and community applications and for encryption of data.

14.1 Platform-centric approach

In the first approach, the client is able to talk directly to three platforms (each providing communication, community and PICOS functionality respectively).

The community platform is responsible for managing content, and higher level communication and context (location) services.

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

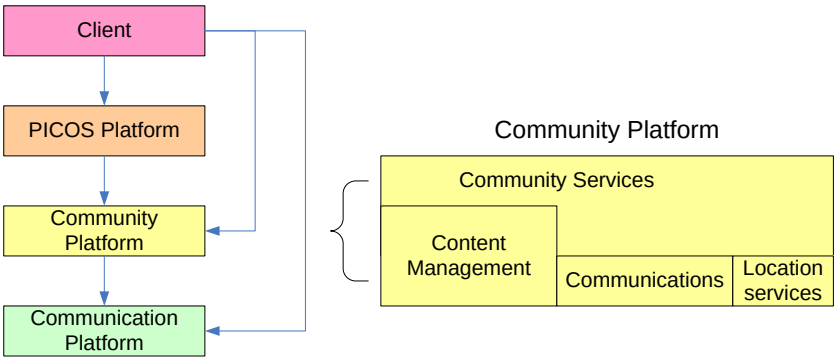


Figure 39 Platform-centric implementation

The communication platform handles all communications between client and the community platform. For example, this service might be provided by a (mobile) network operator.

The PICOS platform hosts the privacy, trust and identity management functionality that PICOS offers.

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

14.2 Services-centric approach

An alternative approach is to look at the implementation from the perspective of services. A (mobile) client interacts first with an application, which in turn draws on services provided by a community platform or the PICOS enhancements. Additional services are supplied by external service providers.

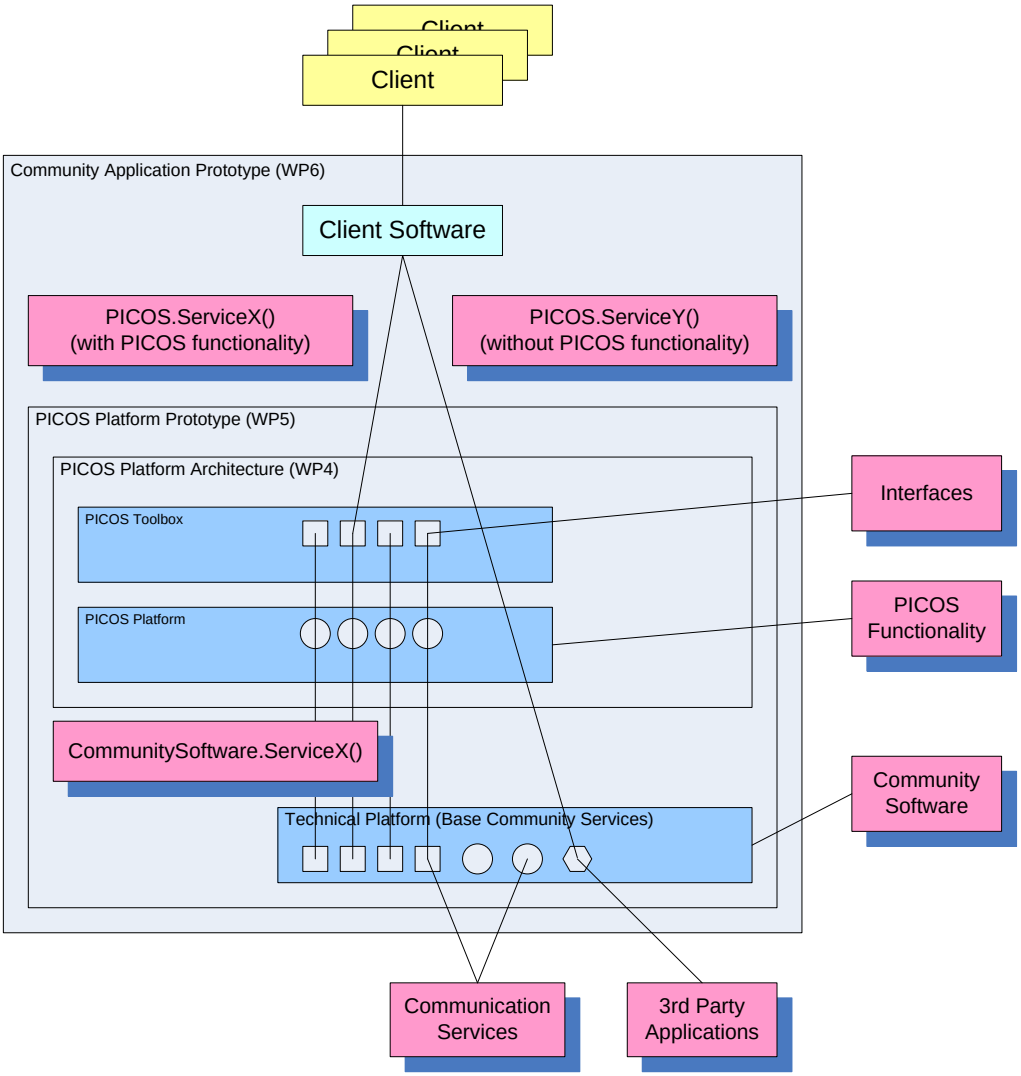


Figure 40 Services-centric implementation

Other configurations are possible. In practice, the hardware may support more than one platform type, or the services may be distributed across several platforms.

In the sub-section on topologies we suggest that client-service is not the only option. A peer-to-peer configuration, which offers some attraction to members who are at the less trusting (low trust) ending of the trust spectrum, would position more functionality at the client. Another possibility is a hybrid,

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

or pseudo-P2P configuration, in which P2P services are routed via a central hub (e.g. the community operator).

Since this architecture is essentially services-based, it can be visualised as a set of service deliveries hosted outside of the core community platform, thus:

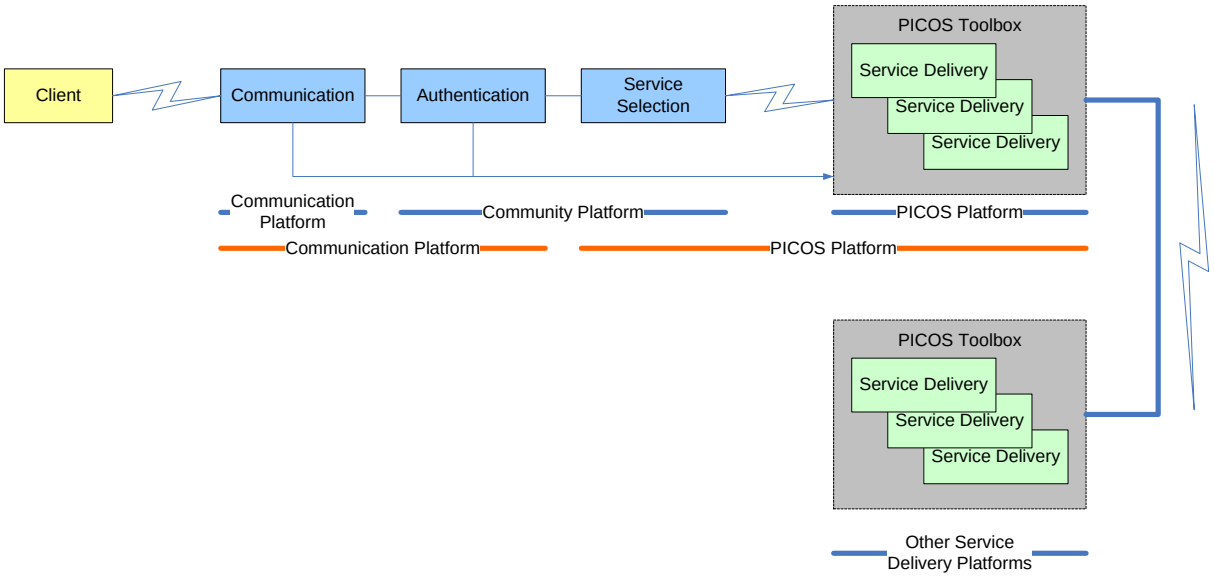


Figure 41 Simplified services-based architecture

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

15 Bibliography & References

[ACM] Social Networks via Viral Marketing, Communications of the ACM (46:12), pp. 300-307

[Albers, Kahl, 2008] Albers, Andreas; Kahl, Christian (2008) Prototypical Implementation of an Intermediary Platform for Context-sensitive Mobile Marketing Applications, In: Proceedings of the 14th Americas Conference on Information Systems (AMCIS), Toronto, Canada.

[Beals, 2010] Beales, H. (2010) The Value of Behavioral Targeting (Study), Networked Advertising Initative.

[Caroll, 2007] Carroll, Evan (2007) Success Factors of Online Social Networks, The University of North Carolina, Chapel Hill, USA.

[Chew et al, 2009] Chew, Monica; Balfanz, Dirk; Laurie, Ben (2008) (Under)mining Privacy in Social Networks, *In:* Proceedings of W2SP 2009 Web 20 Security and *Privacy*.

[Dobele et al, 2005] Dobele, A., Toleman, D., & Beverland, M. (2005), "Controlled infection! Spreading the brand message through viral marketing", Business Horizons, 48(2), March-April, pp.143-149.

[Dobele et al, 2007] Dobele, Angela; Lindgreen, Adam; Beverland, Michael; Vanhamme, Joelle; van Wijk, Robert (2007) Why pass on viral messages? Because they connect emotionally, In: Business Horizons, Elsevier, Vol. 50 (4), pp. 291-304.

[Duncan, Moriarty, 1998] Duncan, T. and Moriarty, S.E. (1998), A communication-based marketing model for managing relationships", Journal of Marketing, Vol. 56 No. 2, pp. 1-13.

[Facebook] Facebook Advertising, www.facebook.com/advertising

[Foursquare] Foursquare, http://foursquare.com/businesses/

[Ho, 2009] Ho, S.Y. (2009) Opportunities and challenges of mobile personalization: An exploratory study. In: Newell S.; Whitley E.A.; Pouloudi N.; Wareham J.; Mathiassen L. (Eds.) Proceedings of 17th European Conference on Information Systems (ECIS 2009), 1211-1222, Verona, Italy.

[Ho, Kwok, 2002] Ho, S.Y.; Kwok, S.H. (2002) The Attraction of Personalized Service for Users in Mobile Commerce: An Empirical Study, In: ACM SIGecom Exchanges, Vol.3 No.4, pp. 10-18.

[Hoegg, 2006] Hoegg, R. et al. Overview of business models for Web 2.0 communities. In Proceedings of Workshop ‘Gemeinschaften in Neuen Medien (GeNeMe)’, TUDPress, Dresden, 2006, 33-49.

[Hristova, O’Hare, 2005] Hristova, N., and O’Hare, G.M.P. (2005) Ad-me: Wireless Advertising Adapted to the User Location, Device and Emotions, *Proceedings of*

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

	37th Hawaii International Conference on System Sciences, Hawaii, USA.
[IDC, 2008]	IDC Report. U.S. Consumer Online Attitudes Survey Results, Part III: Social Networking. IDC, 2008. (http://www.idc.com/getdoc.jsp?containerId=214899); Retrieved on 2010-06-08
[Kahl, Albers, 2010]	Kahl, Christian; Albers, Andreas (2010) Towards reasonable Revenue Streams through Marketing in Mobile Social Networks, In: Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI), Göttingen, Germany.
[Kollmann, 2006]	Kollmann, Tobias (2006) E-Venture, 1st Edition, Gabler, Germany.
[Kotler, Arnstrong, 2006]	Kotler, P, Armstrong, G (2006) Principles of Marketing. 11th Edn, Prentice Hall, New Jersey, Upper Saddle River, USA.
[Kruchten, 1995]	Kruchten, Philippe (1995), Architectural Blueprints — The "4+1" View Model of Software Architecture. IEEE Software 12 (6), pp. 42-50
[Kurkovsky, Harihar, 2006]	Kurkovsky, S., and Harihar, K. (2006) Using ubiquitous computing in interactive mobile marketing, *Pers Ubiquit Compt*, 10,1, 227-240.
[Liesebach, Scherner, 2008]	Liesebach, Katja; Scherner, Tobias (2008), *D2.4 Requirements*, Public Deliverable of EU Project PICOS, November 2008, Available at http://picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/D2.4%20 Requirements/ D24_requirements_final_version.pdf.
[Linkshare, 2009]	Study on Social Network Adertisements. Linkshare, 2009. Tetrieved on 2010-06-08 (http://www.netimperative.com/news/2009/august/social-network-ads-2018failing-to-engage-users2019)
[Loopt]	Loopt Star, http://www.loopt.com/looptstar
[Nielsen, 2009]	Global Faces and Networked Places (Study). Nielsen, 2009.
[OFT, 2010]	Office of Fair Trading (2010) Online Targeting of Advertising and Prices (Study), London, England.
[Palmer, Koenig-Lewis, 2009]	Palmer, Adrian; Koenig-Lewis, Nicole (2009) An experiential, social network-based approach to direct marketing, Direct Marketing: An International Journal, Vol. 3 No. 3, pp. 162 – 176
[Phelps et al, 2004]	Phelps, J.E., Lewis, R., Mobilio, L., Perry, D. and Raman, N. (2004) Viral Marketing or Electronic Word-of-Mouth Advertising: Examining Consumer Responses and Motivations to Pass Along Email, In: Journal of Advertising Research, vol.44 no.4, pp.333-348.
[PICOS 1, 2007]	PICOS Grant Agreement - Annex 1, B1.1.2, 2007.
[PICOS 2, 2007]	PICOS Grant Agreement - Annex 1, B1.1.4, 2007.
[Pousttchi et al]	Pousttchi, K; Turowski, K.; Wiedemann, D.G (2008) Mobile Viral Marketing - Ein State of the Art, In: Bauer, H.H.; Dirks, T; Bryant, M.D.

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

(Hrsg.): Erfolgsfaktoren des Mobile Marketing. Strategien, Konzepte und Instrumente. Springer, Berlin, S. 289–304.

[Schmidt et al, 1998] Schmidt, A.; Beigl, M.; Gellersen, H.-W.: There is more to Context than Location. In: Computers and Graphics, Vol. 23, 1998. S. 893-901.

[Schulz et al, 2007] Schulz, Sebastian, Mau, Gunnar & Löffler, Stella (2007). Virales Marketing im Web 2.0, in: T. Kilian, B. Hass & G. Walsh (Hg.). Web 2.0 – Neue Perspektiven im E-Business, Heidelberg: Springer, pp. 249-268.

[Subramani, Rajagopalan, 2003] Subramani, M.; Rajagopalan, B. (2003) Knowledge Sharing and Influence in Online

[Verlag] Commercialisation of Context-sensitive Mobile Attention in Mobile Media Markets - Design Recommendations for Mobile Marketing Providers, Schriften zum Mobile Commerce und zum Mobilfunk, Verlag Dr. Kovač, Hamburg, Germany (Forthcoming).

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

Appendix A Use Cases

This appendix describes in detail the use cases that influenced the architecture. PUC1 – PUC9 are directly imported from D4.1; PUC16 – PUC23 are new to D4.2. (As mentioned in the body of this deliverable, PUC10 – PUC15 first mentioned in D4.1 were not considered further in D4.2.)

A.1 PUC 1: Registration

A.1.1 Situation

All members of the community must be registered if they wish to have full access to the facilities on offer. Guests, who may be considered anonymous members, are an exception to the registration rule, since registration is not necessary, but the range of services available to a Guest is severely restricted. In order to gain access to the full range of services, registration is necessary.

Registration provides the community operator with assurance that a member is suitable to join the community. This assurance may be through prior knowledge of the member, or through evidence that minimises risks to the community (e.g. the real name and address of the prospective member, which provides a route to compensation if required).

Obviously, new 'unknown' members must be able to join the community, and for this PICOS offers an 'application process' (e.g. application form) where applicants provide information requested by the community operator and are granted membership if they meet the requirements set by the community operator or elected member representatives.

Every member is allocated a root identity. The root identity is only used for registration and to link subsequently created partial identities. The root identity is only known to the community operator, and is linked to the registration information (which in most cases will ultimately be a real name and address).

In order to interact with the community, each member must create a partial identity (a pseudonym). They can create any many partial identities as they feel they need, but they must create at least one. Creation of the first partial identity would normally take place at the time of registration, but can occur later.

Every partial identity is allocated a feedback pseudonym. The feedback pseudonym enables members to provide feedback to the community without revealing their partial identity.

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

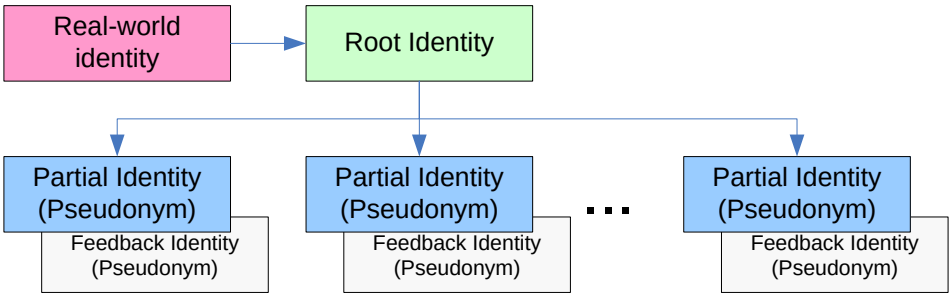


Figure 42 Root and Partial Identity overview

To summarise, every member has one root identity which is assigned when they register with the community. They are immediately allocated a partial identity when they first interact with the community. All identities, including root, have a profile, but only partial identities have feedback identities. A member can only have one root identity. Roles other than member, e.g. community administrator, are treated as special cases.

Optionally, a member can create further pseudonyms at the time of registering. Just like the first partial identity, each subsequent partial identity is assigned a feedback pseudonym[12].

Pre-registered identities are also accepted by the community. For example, a member who is already registered with a mobile phone provider may be permitted to use the allocated identity as their community root identity, so long as the member consents to this. This situation is particularly useful where a community is hosted by the telecoms provider.

[12] The diagram shows two levels of identity (Root and Partial) where all partial identities are directly linked to the root identity. We recognise that partial identities may also spawn partial identities, creating a tree-like structure. To date we have not seen a need for this approach, but we keep it in mind should a need arise.

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

A.1.2 Reference diagram

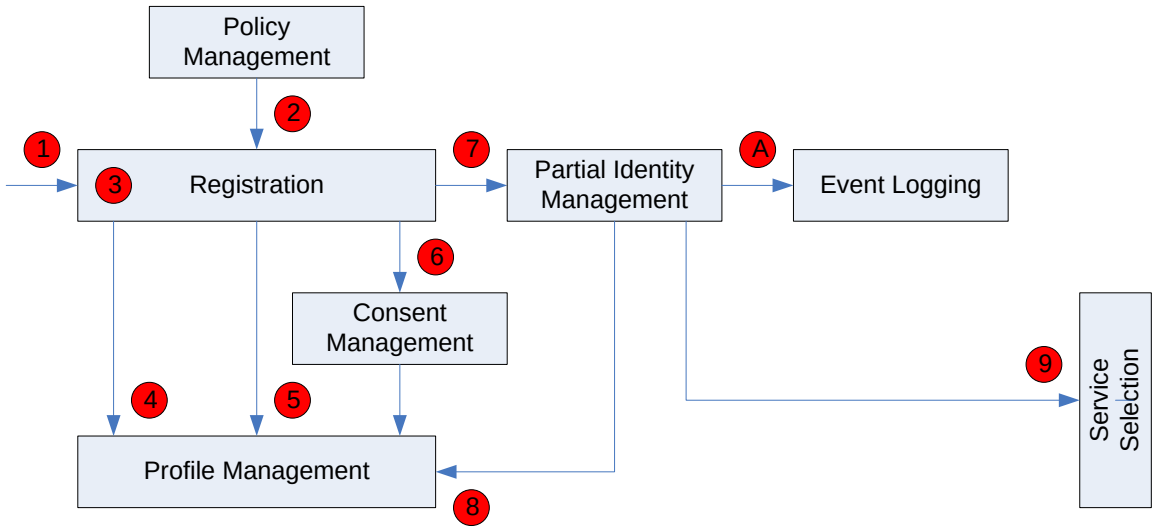


Figure 43 PUC 1: Registration

A.1.3 Walk-through

A prospective member approaches the community and presents to the *Registration* component {1} evidence of one or more of the following[13]:

- prior registration with a real-world community
- prior registration with a mobile phone network provider
- prior registration with a 'partner' community
- another acceptable credential as defined by the community policy
- successful completion of the application process (e.g. application form)

The choice of what is considered an acceptable form of registration is notified by the *Policy Management* component {2}.

The *Registration* component assigns a root identity {3}, and records this alongside the evidence that the member provided in the member's profile using the *Profile Management* component {4}. Registration also assigns a default role and privileges to the new member {5}.

Once registered, the member can set certain elements of their personal profile to help manage privacy using the Consent Management component {6}.

Following registration, the member creates their first (and possibly only) partial identity, which they subsequently use to interact with the community {7}. Every partial identity has a unique profile which

[13] We recognise that other forms of registration may be possible and conclude that this list is not exhaustive.

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

holds information about the new identity, e.g. reputation {8}. (The member can also set consent preferences for the new identity, but for clarity this is not shown in the diagram. See PUC covering Multiple (partial) identities.)

Once a partial identity has been assigned, the member can access the service {9}.

All actions performed are logged by the *Event Logging* component {A}.

A.1.4 Reference to the User Scenario

Before John can access the services he must first register. This involves John providing supporting evidence to authenticate his identity, some of which is personal information. The evidence that John sends is actually a credential issued by a governmental fishing authority.

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

A.2 PUC 2: Accessing the community

A.2.1 Situation

Having first registered with a community, a member can then access the community to call on the services offered by the community.

Accessing the community involves presenting a partial identity and supporting authentication information. Once authorised, a member is able to select the required service from those provided by the PICOS community application. The process of accessing the community assigns pre-set privileges to the member and can reveal their status (presence) to other members subject to the member giving consent.

A.2.2 Reference diagram

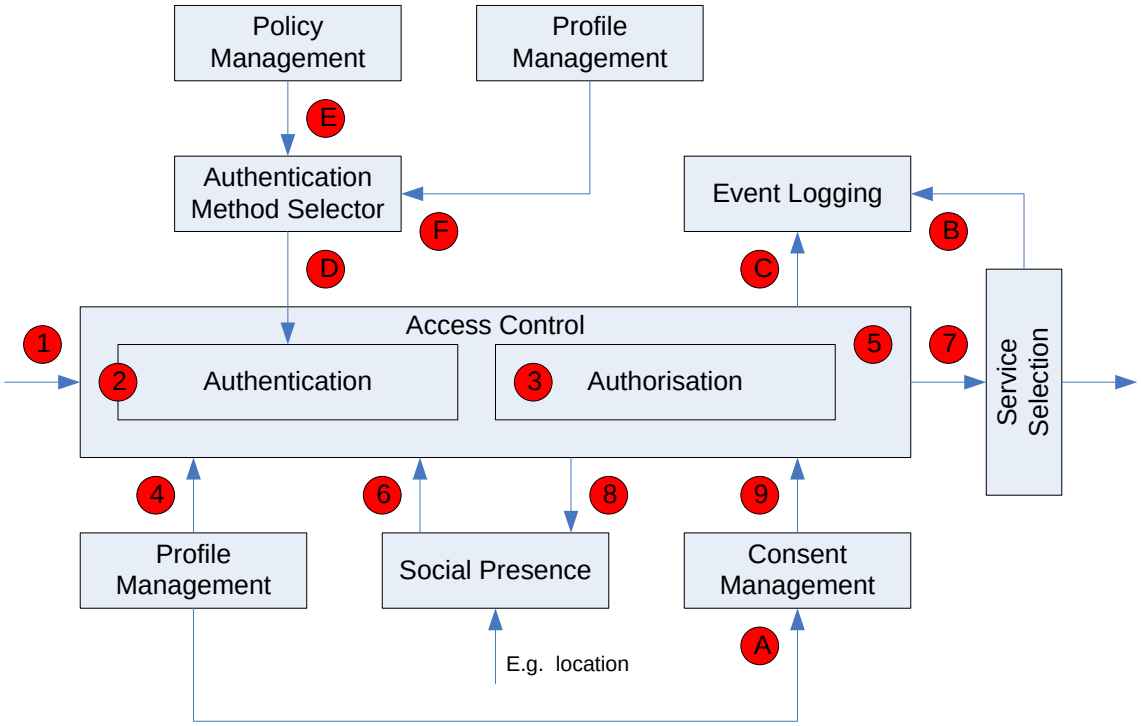


Figure 44 PUC 2: Access control

A.2.3 Walk-through

The member presents their partial identity via the Access Control component {1} and authentication information to the *Authentication* component {2}. The method of authentication is indicated by the Authentication Method Selection component {D}, which takes input from the community policy and

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

the member profile, via the Policy {E} and Profile Management {F} components respectively. This means that either the community can dictate the method of authentication for all members, or each member can select a preferred method. The community policy would typically indicate a range of acceptable authentication methods, leaving the member to choose the preferred method, perhaps taking into account data minimisation concerns. If accepted, they are authorised {3} and allocated privileges by the *Personal Profile Management* component according to their role {4}.

Member privileges dictate the access that a member has within a community. The *Access Control* component determines the set of services that the member can access {5} by checking the member profile {4}, taking into account any context information like social presence {6}. Available services are then presented to the member {7}. At the same time, a member's social presence is updated to show to other members that they are active within the community {8}, assuming that they have given consent as defined by the Consent Management component {9} and available through the Profile management component {A}.

All actions performed are logged by the *Event Logging* component {B}{C}.

A.2.4 Reference to the User Scenario

After registering, John accesses the community. He previously created a profile that defines personal attributes (e.g. buddy list) and personal interests. The profile also let John set preferences that define who can see his personal status (presence).

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

A.3 PUC 3: Revocation

A.3.1 Situation

Revocation occurs when members leave a community for the final time. This may occur through choice or because the community has terminated the member's membership. In addition to denying the member further access to the community, the community operator must take action with respect to content that was contributed to the community during the lifetime of the membership.

Content is handled in several ways, depending on the policy set for the community:

- Removed from the community (Probably default position)
- Retained in the community for other members to (continue to) access

There are multiple reasons for retaining content: 1) legislation dictates so, 2) content is still useful to the community (e.g. reputation), 3) content can be transferred to another member or the community operator.

Where content is retained by the community, the most likely action will be to pseudonymise the identity of the contributing member. This will satisfy both legal requirements and member revocation preferences. The decision to 'anonymise' or destroy may depend on the nature of the content. For example, personal data may need to be destroyed in order for the community to comply with EU Data Protection legislation. It may be acceptable for other content to be destroyed.

There is a possibility that a member may choose to return to the community. If this is a concern, then the community policy will state whether reputation information (and possible other content subject to Data Protection Law and the need to only retain information that is relevant and not excessive), and presumably the real identity of the member to who it related, can be retained. Options are that reputation is deleted or frozen/suspended.

We have already mentioned that event and audit services require special attention if privacy it to be maintained. If retained, or removed and archived, content may need to be anonymised.

The process for deciding which of the above options is appropriate will depend on the needs of the individual, the community and legislation, as stated in the community policy.

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

A.3.2 Reference diagram

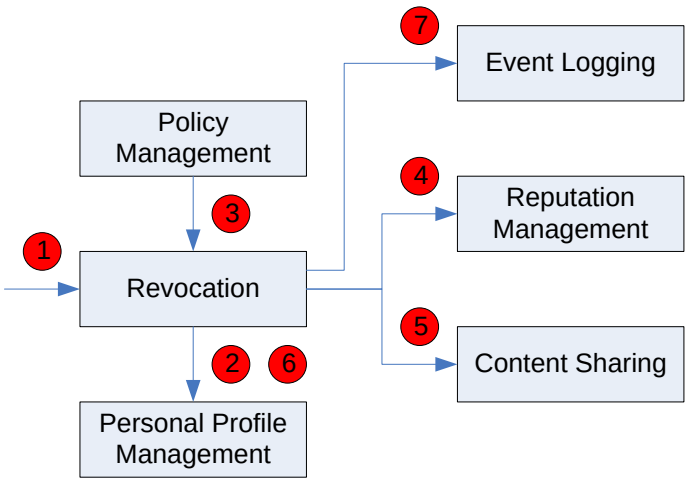


Figure 45 PUC 3: Revocation

A.3.3 Walk-through

The *Revocation* component is responsible for terminating membership. Revocation would normally be initiated by the community operator {1}.

The first step in the revocation process is for the member profile to be set to deny further access to the community by the member {2}. This may affect the root identity and all partial identities, or just the partial identity in question. Thus authorisation will fail if the terminated identity attempts to regain access.

According to community policy, as communicated by the *Policy Management* component, content for each and every identity affected by the termination will be either destroyed, archived or anonymised {3}. Responsibility for this decision lies with the *Revocation* component, which will trigger appropriate action {4} {5}.

The feedback pseudonym, which would have been created if the member provided feedback from their root and/or partial identities, can remain and will ensure that feedback is present for future inspection by members. The profile of each feedback pseudonym will show 'membership terminated' {6}. The profile of the member may also show the reason for leaving community, e.g. 'resigned', 'terminated', 'excluded'. A member who leaves the community voluntarily would have a different reason recorded than a member whose membership was terminated by the community manager due to (say) bad behaviour. The reputation might also be downgraded if the member was asked to leave the community, possibly to a special reputation value, e.g. a dash/hyphen.

All actions performed are logged by the *Event Logging* component {7}.

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

A.3.4 Reference to the User Scenario

When John decides to leave the community he cancels his membership, but history of his membership and messages he has posted remain.

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

A.4 PUC 4: Multiple partial identities

A.4.1 Situation

In addition to partial identity created when a member registers with the community, a member may create one or more additional partial identities (or pseudonyms). The reason that this facility is provided is to allow a member to represent themselves in different ways within a sub-community, or across multiple sub-communities. It means that each partial identity can potentially gain a different level of respect (reputation) depending on their interaction with the sub-community(ies). For example, a member may be an expert on fly fishing, and thus willing to provide advice and help to others using one partial identity. However, they may also be just learning about sea fishing and do not want to present the same partial identity for fear that it may lessen the respect that they have in the fly fishing community. In such a case, the member chooses the most suitable partial identity depending on whether they are interacting with the fly fishing sub-community or sea fishing sub-community.

Each partial identity can be used to access one or more sub-communities. For example, a member may have three partial identities that each access the same sub-community, or they may have five partial identities that access five sub-communities (one partial identity per sub-community). Other permutations are equally possible. Essentially, any partial identity can access any sub-community(ies) assuming that the owner (creator) of the sub-community grants permission.

Each member partial identity appears to all other members as a unique, individual member. Only the community operator knows the true link between root and partial identity(ies).

Every partial identity has an associated feedback identity, which is used to provide feedback (including reputation), and a personal profile (which records a member's reputation). When a member provides feedback and/or reputation, they do so anonymously. The member may want to be anonymous because that are worried that if they are truthful and provide negative feedback they may feel threatened. (Extreme examples are e-voting and 'whistle blowing', e.g. a police informer.)

However, the member receiving the feedback wants to know who provided the feedback, so that they have some confidence that the feedback is honest and fair. Further, an 'observing' member wants to have faith in the reputation system as a whole. For example, on eBay a buyer probably has no idea who the seller and previous purchasers are, and has only the reputation system to help decide.

At a technical level, partial and feedback identities are identical. They both are unique values within the community. There should be no linkability between partial identifies, or between partial and feedback identities (accepting that in the initial trust model this will be possible at the community operator level). Feedback identities do not need to be visible to any other members. They could be randomly generated values, produced by the system when the partial identity is created, and remain an internal 'system value'.

Feedback identities allow members to provide 'anonymous' feedback and reputation. The fact that feedback identities are actually pseudonymous (i.e. know to the community operator) means that there is some control over how feedback is provided, and consequently higher confidence in the reputation system as a whole.

While members who provide feedback cannot be personally identified, certain attributes about them can be determined. For example, a member can only provide feedback once. If they have ten partial

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

identities, they can only use one to provide feedback (specifically reputation) on another member. The linkability achieved through the member's root identity enables the community operator to police this community policy restriction. The reputation of the member providing the feedback can also be revealed, as too can an aggregated reputation (root identity reputation), which is based on the reputation of all partial identities under a single root identity. Thus, without revealing the partial identity, it is possible to gain a strong feeling about the member who is providing feedback. Other factors help build confidence in the reputation system, for example members join the community through a strong registration process.

Members who are comfortable revealing their partial identity when providing feedback are also catered for. Members can add their true/real identity in the profile of a partial identity, if they chose, but it is also possible for a member to select the 'non-default' option to publicly link their partial and feedback identities in the feedback provided. This may be an attractive option for a sub-community administrator, or for someone which a high real-world reputation.

A community member who has multiple partial identities may want to be recognized for his achievements in united way. Therefore it may be reasonable in certain situation for the member to merge previously created partial identities. For example, as a member obtains a higher level of expertise/reputation in sea fishing, he may want to be recognized under single partial entity in both fly and sea fishing communities.

PUC5 discusses reputation in more detail.

A.4.2 Reference diagram

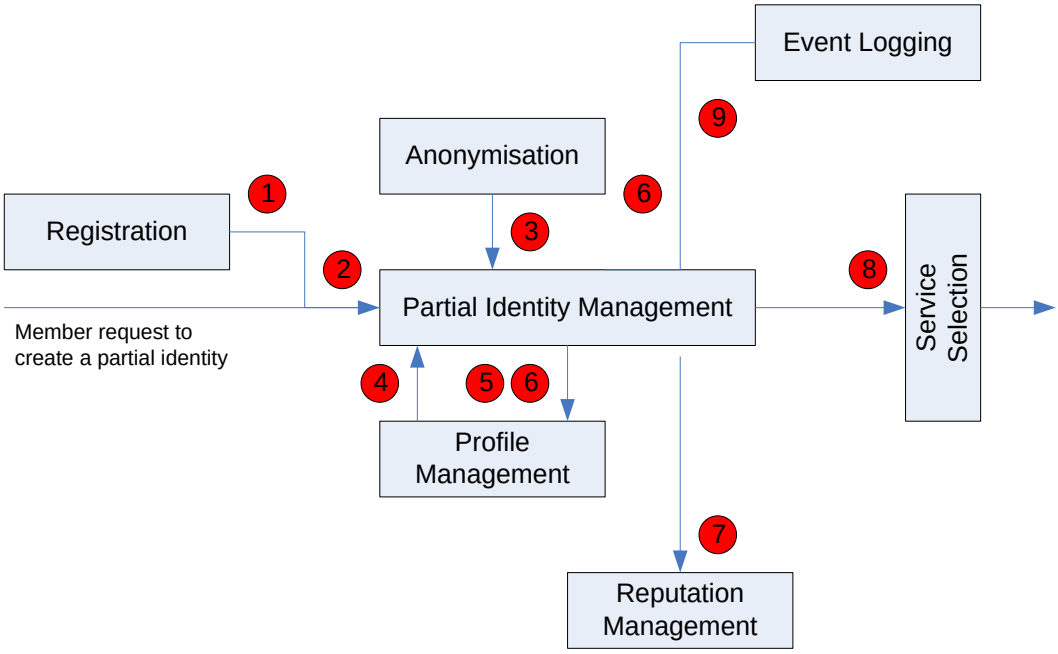


Figure 46 PUC 4: Multiple partial identities

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

A.4.3 Walk-through

Once registered with a community, a member can create one or more partial identities. Each partial identity is registered with the community. (Note: When a member first registers, the *Registration* component calls the Partial Identifier component to create the first partial identity {1}.)

Partial identity creation is a service available to members through the *Partial Identity Management* component {2}. Every partial identity must be unique. The identity can be chosen by the member (so long as it is unique) but will more likely be automatically created by the *Anonymisation* component {3}. (Member-chosen identities may reveal the real identity of the member and should be discouraged. If members wish to identify themselves through their partial identity then they can include a photo or a name in the partial identity profile, and then selectively reveal this information to others members. {4})

The new partial identity adopts the privileges of the root identity {5}, but these can subsequently be modified (reduced) by the member through the Profile Management component {6}. The reputation of the partial identity would most probably set to a default 'neutral' value {7}, or preferably might inherit the reputation of the root identity (which is the 'average' of all partial identities linked to the root identity).

As currently envisaged, all partial identities are directly linked to a single root identity. A partial identity cannot be linked to another partial identity (but see Footnote to PUC 1).

Once a partial identity has been created, the member can use the new identity to interact with the community and select services available {8}.

It is also possible for a member to import a partial identity from another community. There are some limitations, e.g. both communities must operate compatible identity and reputation management systems, but in principle importing should be possible.

All actions performed are logged by the *Event Logging* component {9}.

A.4.4 Reference to the User Scenario

John creates two partial identities, one for his fishing holiday and another for fly-fishing.

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

A.5 PUC 5: Reputation

A.5.1 Situation

Reputation is a reflection on the ability of an entity (normally a member, but also content, an asset, an external service provider or sub-community) to satisfy the values that a community maintains. It is directly related to trust. Reputation involves two processes: 1) providing information that builds a reputation, and 2) retrieving the reputation of an entity. In addition, members wish to contribute reputation anonymously while still being able to rely on (trust) reputation received. In practice, this means receiving assurance that reputation is provided by an authorised member of a sub-community, and that a level of accountability exists.

Members should also be able to 'link' items of feedback – a member may consider that feedback pseudonym 'xyz' provides feedback that they find particularly useful. This is one reason why the feedback pseudonym for a given partial identity never changes. Every feedback pseudonym has a profile.

Every partial identity has reputation, but so too does the root identity. Root identity reputation helps members understand the member behind the partial identity. Take a member who has two partial identities, one with a good reputation and the other with a bad reputation. It is arguably useful for members to know that these two reputations relate to the same members, but unlinkability prevents this. Although root identities are not visible to the membership, its reputation can be provided in such way that it 'averages' all partial identities under that root identity. The exact process is the subject of further research.

Members can provide feedback using each of their partial identities (pseudonyms). In each case, feedback is recorded under the corresponding partial identity feedback pseudonym. An exception is where a member can only provide feedback once, e.g. when voting. A member can provide feedback (textural comments) more than once, but can only comment on reputation once. However, reputation values can be edited if the contributing member wishes to revise their opinion.

Reputation can also relate to external services providers. Here, every service provider is assigned a partial identity which attracts a reputation value when members provide feedback. The service provider cannot influence the reputation value themselves. Third parties can also provide feedback on service providers. This might result from a trusted independent review (e.g. audit, consumer body) of the service providers operation, and their ability and willingness to comply with legislation.

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

A.5.2 Reference diagram

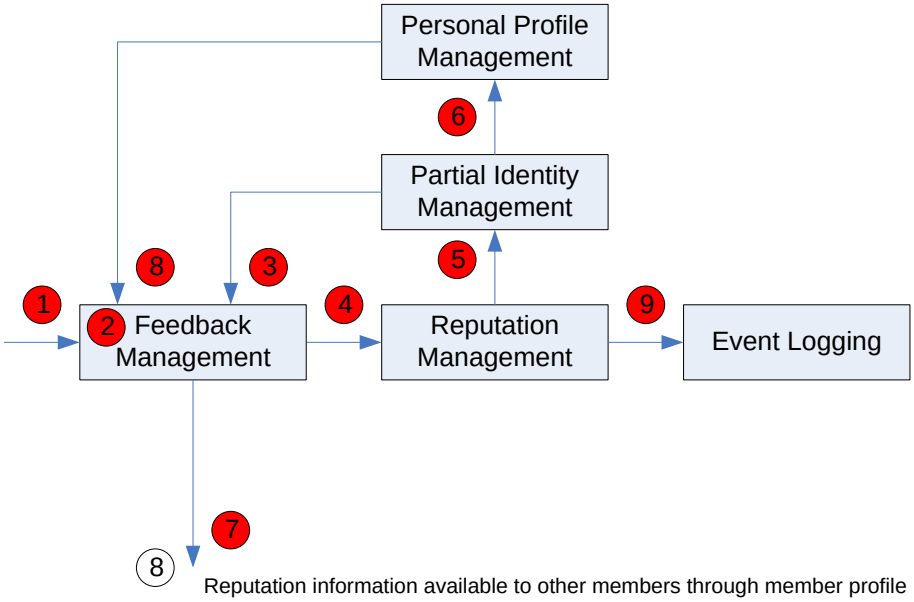


Figure 47 PUC 5: Reputation

A.5.3 Walk-through

Reputation is received from members through the *Feedback Management* component {1}. This component allows members to select the entity {2} that they wish to provide feedback on, and prompts for a reputation indicator (e.g. on a scale of 1-5). Entity identities are obtained from the *Partial Identity Management* component {3} and passed to the *Reputation Management* component {4}, where the feedback pseudonym associated with the partial identity (of the contributing member) is located and {5}, and returned to the *Profile Management* component {6} where they are recorded in the profile of the entity to which it relates (normally a member).

The feedback pseudonym is a 'special' pseudonym that ensures contributing members are not identified to other members. However, it is important that the reputation service is not open to abuse. Therefore, feedback is provided under a pseudonym which allows the community operator to inspect the member root identity if necessary. The feedback pseudonym is created when the member first uses the feedback service.

Reputation is a read-only value that cannot be modified except by the reputation service or the community operator. When a member inspects the profile of a member they will see their reputation {7}. Other services that rely on reputation can also inspect the profile value. For example, in some situations, reputation can only be provided by members who have a positive or neutral value, in which case the reputation service will block feedback from members who have a negative reputation {8}.

All actions performed are logged by the *Event Logging* component {9}.

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

A.5.4 Reference to the User Scenario

John uses the reputation service to check the reliability of information he uses to plan his trip. He also establishes a personal reputation, which he leaves with the community when he cancels his membership.

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

A.6 PUC 6: External services

A.6.1 Situation

The PICOS community supports a wide range of service. However, there will be times when a community requires a specific service that is provided by another 'external' community. For example, the angling community may require road or rail information in order to plan a fishing trip.

External services raise two sets of concerns, namely:

- Privacy
- Accuracy and reliability

External communities are represented within the community just like any other entity (i.e. member, resource). Every service has a locally maintained profile which contains the reputation information. Consequently, every service provided has a partial identifier against which reputation is recorded. In the case of a service provider, it may be desirable for the partial identity to actually name the provider (which is possible, though not advisable for ordinary members, because entities can choose a partial identity so long as it is unique within the community).

The selection of an external service triggers a request to the External Service Delivery component, which acts as a proxy for the external service.

Privacy

When a member accesses an external service, they do so under a partial identity (pseudonym). This special 'external services' partial identity is created automatically by the community 'on demand', in a similar way to which a standard partial identity is created under the member's root identity.

Accuracy and reliability

The accuracy and reliability of an external service is described by the service's reputation. Just like entities within the community, external services carry a reputation indicator that has been compiled by all communities that use the service, according to a standardised format for expressing and sharing reputation information. In addition, feedback information is available, although the quality of this information depends on the nature of the contributing community and its alignment (in terms of members' interests) with the local community.

Members can check the reputation of an external service using the Personal Profile Management component. This component returns the reputation to the member.

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

A.6.2 Reference diagram

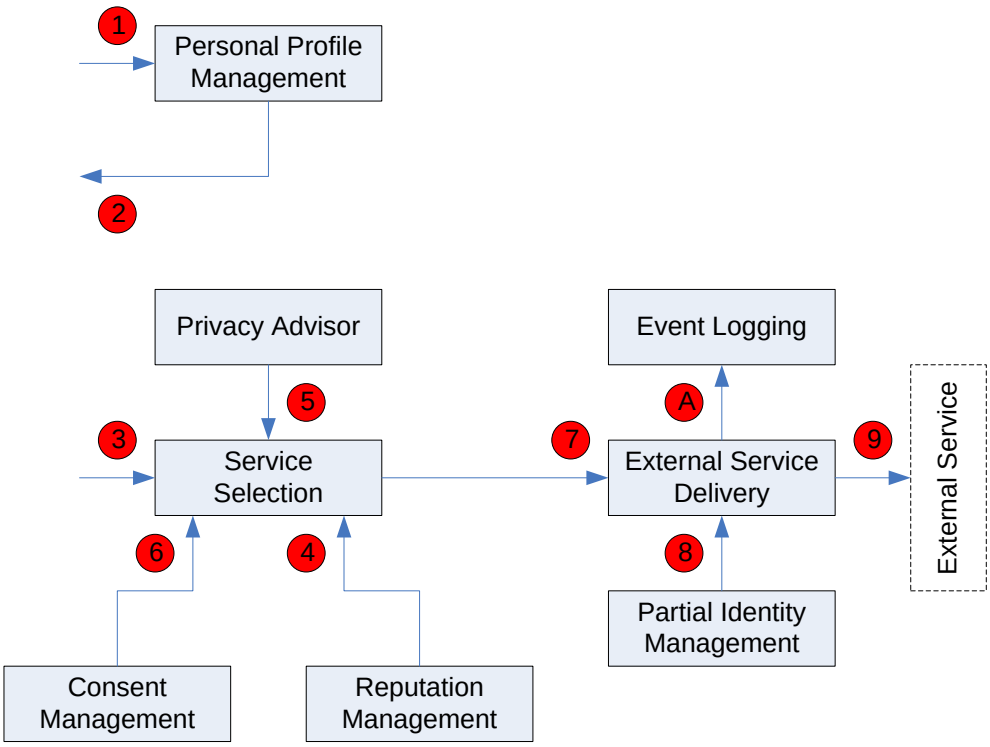


Figure 48 PUC 6: External services

A.6.3 Walk-through

A member requests the reputation of an external service by selecting the entity identity from the *Personal Profile Management* component {1}. This component returns the reputation {2}.

An external service is selected in the same way as an internal PICOS service, except that it is accessed via a proxy {3}.

Prior to selecting a service, a member can inspect the reputation of the service provider {4} and obtain privacy advice from the *Privacy Advisor* component {5}.

The choice of whether a member shares their partial identity and other personal information with the service provider is stipulated on the consent that the member has given, and is available through the Consent Management component {6}.

The external service is accessed through the *External Service Deliver* component {7}, which calls the *Anonymiser* component if members have stated that they do not want to share their partial identity {8}. The *Anonymisation* component generates a pseudonym 'on-the-fly'. This pseudonym is shared with the external service {9}.

All actions performed are logged by the *Event Logging* component {A}.

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

A.6.4 Reference to the User Scenario

John uses external services to check weather and biological information from FishBase. Access to the external services is described in the scenario as using Federated Identities. At present we do not have a use case covering federated access.

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

A.7 PUC 7: Content sharing

A.7.1 Situation

Members can contribute content, which includes all types of member generated data, e.g. text, video, (recorded) voice and images, to the community. This is called importing. Members can also remove (copy) content from the community, which is called exporting. The import/export component co-ordinates both activities. For example, the *Import/Export* component identifies the source (or name) of a photography that is to be imported.

Content is always associated with the identity of the member who performed the import, which can be a partial identity. When imported, content is tagged (i.e. attributes, or meta-data, are attached) to help identify the content to other member of the community. Certain tags are assigned by the contributing member, while others are derived by the community. For example, member tags may include description, sharing options and target community, while community tags include contributing member reputation (but not necessarily identity). The *Content Sharing* component is responsible for associating tags with content.

Once content has been successfully imported, the content is available for others members to view (subject to matching the profile stated by the importing member). Optionally, the importing member may actively notify other members (push) using the *Notification* component. The decision to notify or not is taken at the time of import, or is set in the importing member's profile.

Members must be connected to the community and authorised to access the import/export service in order to perform this action.

Tagging is a complex subject that requires further research. For example, members are likely to want to tag content, especially photographs, with the identity of the subject. This can be useful since it provides an opportunity to notify the subject (assuming that they are a member of the community) that a photograph of them is visible to the community. This only works if a valid identity is selected; if free format tags are permitted, then analysing tags is more complicated. The reality is that members would probably prefer free format tags. A partial solution is to notify all members of a sub-community every time any photograph is imported, so that it can be inspected. This is not a convenient solution for members.

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

A.7.2 Reference diagram

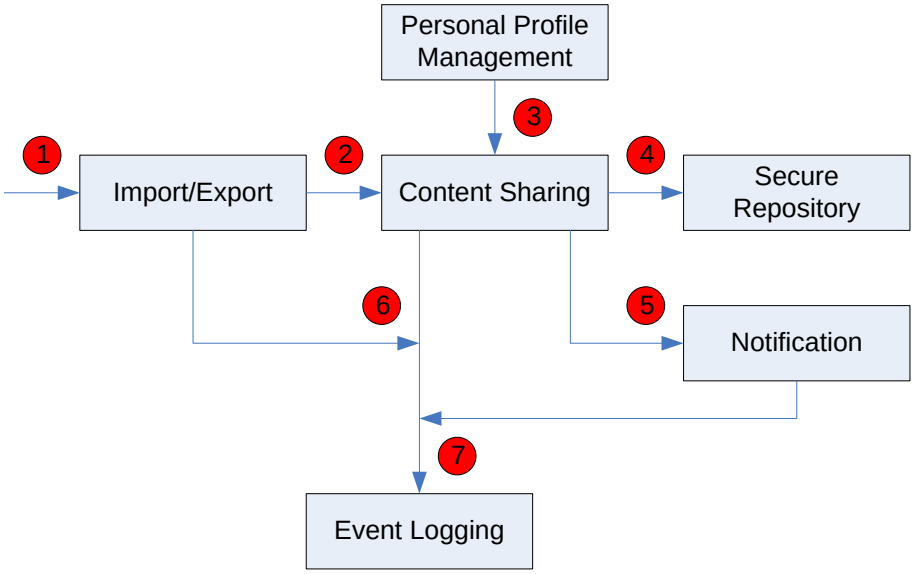


Figure 49 PUC 7: Content sharing

A.7.3 Walk-through

A member, authenticated and authorised by the community, selects the Import/Export service and specifies the source of the content to be imported {1}. Next, the *Content Sharing* component tags the content {2}, taking tag information from the member and the member's profile {3}, and places the tagged content in the content store {4}.

Finally, the *Content Sharing* informs the *Notification* component to issue a notification that new content is available {5}. (Notification can be to the whole community, one or more sub-groups and/or specified members.)

All actions performed are logged by the *Event Logging* component {6} {7}.

A.7.4 Reference to the User Scenario

John is keen to share content. For example, he creates a 'holiday in the Alps' sub-community. When cancelling his membership he is 'rated' (reputation) for his contribution.

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

A.8 PUC 8: Presence

A.8.1 Situation

The status of a member (called social presence) is freely available for other members to see unless the member concerned chooses to deny access to all or part of their presence information.

Presence describes a member's current situation, e.g. 'online', their location, role, sub-group membership.

Presence information is held as part of a member's profile. Every partial identity has a profile. Presence information is partially under the control of the member. For example, a member can choose whether to reveal their identity to other members, possibly using a simply on/off option that links to the *Preference Management* component. However, a member cannot falsify location information. For convenience the choice of whether to display presence information can be set as a preference for each partial identity.

A.8.2 Reference diagram

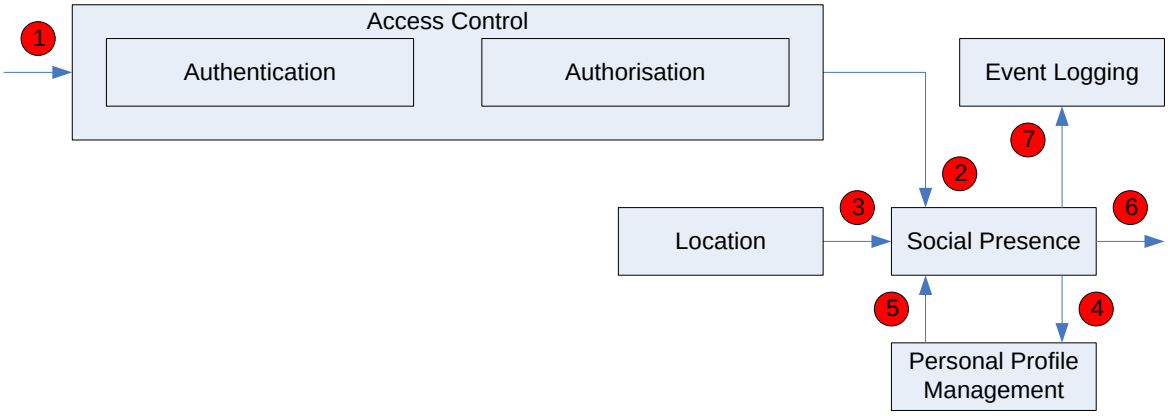


Figure 50 PUC 8: Presence

A.8.3 Walk-through

When a member accesses the community {1} their profile is updated by the *Personal Profile Management* component to reflect their online status and location (and other context information that is considered relevant and is available). The *Access Control* component informs the *Social Presence* component of the change in member status {2}, which in turn triggers the *Social Presence* component to acquire the member location {3} (and other context information).

A member can influence how much information about themselves is revealed to other members, through the setting on their personal profile. Thus, the *Social Presence* component requests {4} this information from the *Personal Profile Management* component, and uses it {5} to set the member's social presence 'filter' before revealing presence information {6}.

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

All actions performed are logged by the *Event Logging* component {7}.

A.8.4 Reference to the User Scenario

John creates several sub-communities, e.g. he creates a 'holiday in the Alps' sub-community which will only be accessibly by members when they are in the Alps on holiday.

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

A.9 PUC 9: Sub-community

A.9.1 Situation

All members belong to the single PICOS community, but each member can create one or more sub-communities. A member selects[14] which sub-community they want to interact with when they connect to the community. As part of the service selection process they can chose one of the sub-communities lists in their profile.

These sub-communities serve a specific purpose identified by the creating member, and can be joined by any member with the permission of the creating member. The creating member can specify individual members, sub-community membership or filter on a set of member personal profile characteristics. For example, a member of the angling community might create a sub-community for anglers interested in using sonar[15] to locate fish.

Sub-communities created in this way take on some of the characteristics of the creating member. For example, the sub-community initially has the same reputation of the creating member. Sub-communities have profiles, just like any other entity, which can record reputation and maintain a list of all sub-community members.

When a member leaves a community, their sub-community(ies) can be deleted, transferred to community operator or delegated to another member. There may also be legal reasons for keeping the sub-community content, even though sub-community is no longer active. Transfer to another owner would require the consent of all sub-group members. Where a sub-group member does not accept the transfer, it must be possible to remove or anonymise their content. Any changes to the sub-community must be notified to all sub-group members.

[14] The number of members with the ability to confirm new members into a sub-community should not be limited to exactly one.
[15] Acronym for SOund NAvigation and Ranging.

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

A.9.2 Reference diagram

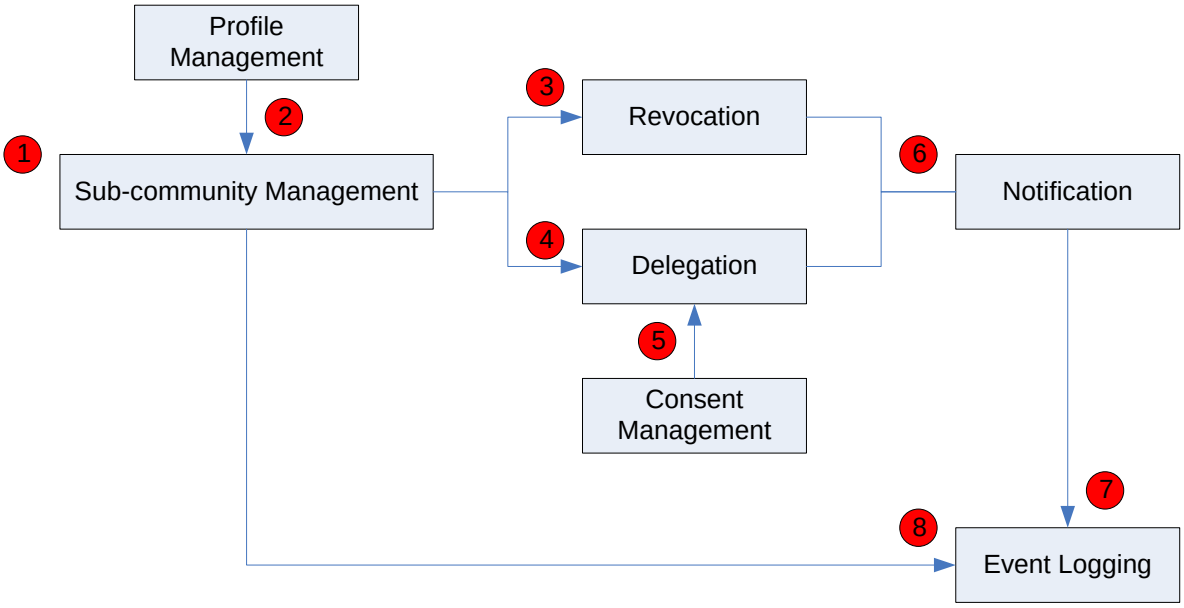


Figure 51 PUC 9: Sub-communities

A.9.3 Walk-through

A member creates a sub-community by issuing a request {1} to the *Sub-community Management* component. As the sub-community is created, it adopts some of the profile properties of the creating member using the *Profile Management* component {2}.

The sub-community is either revoked using the *Revocation* component {3} or delegated using the *Delegation* component {4}. Delegation requires the consent of all sub-group members, obtained through the *Consent Management* component {5}. Whichever action is taken, all sub-group members are told using the *Notification* component {6}

All actions performed are logged by the *Event Logging* component {7} {8}.

A.9.4 Reference to the User Scenario

John creates several sub-communities, e.g. he creates a ‘holiday in the Alps’ sub-community.

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

A.10 PUC 16: Privileges

A.10.1 Situation

Privileges are managed via *roles* defined in particular contexts, e.g. public community, forums, sub-communities. Rules are defined and attached to roles, which are then associated to PICOS resources to form a policy.

The policy component acts as a policy engine that enables the definition of rules, which can include various conditions based on identity, date and reputation.

The policy engine is provisioned using various web service methods that allow the association of rules to resources, the deletion and modification of policies as well as rules in a policy. Each requester creates a "situation" based on the requester Id, the accessed resource and the action to perform on the resource. The policy component checks if there any valid policy to evaluate the "situation" and if any, it replies with the action status that is defined in the rule.

A.10.2 Reference diagram

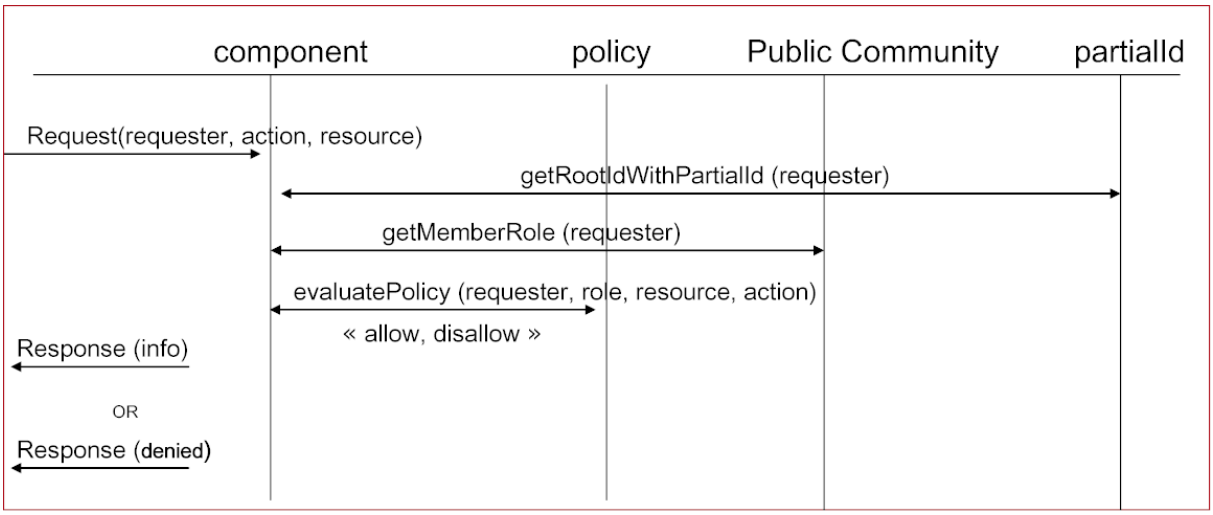


Figure 52 PUC 16: Privileges

A.10.3 Walk-through

For actions like create forum and delete discussion, the privileges are attached to the role of the public community member. As previously implied, the component needs to know the community role of the requester. As the requester may be known by its partial identity, this process must use this identity to obtain the member's role. Once the role is known, the privilege of the requester can be tested.

Where sub-community are involved, the privileges associated with the role relevant to the sub-community must also be assessed.

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

A.11 PUC 17: Multi-communication

A.11.1 Situation

Members/players can communicate with other members/players of their (sub-) communities (or allied players) in order to exchange various kind of primarily game-related information. The communication can be text-based, voice-based or multimedia-based (i.e. pictures or screenshots from within the game). Players communicate in order to discuss and plan their game strategy; results of their strategy after being applied; proper reactions on different in-game situations and, e.g., a coordination of support for other members of their (sub-) communities. The type of communication can be one-to-one, one-to-many, or many-to-many.

A.11.2 Reference diagram

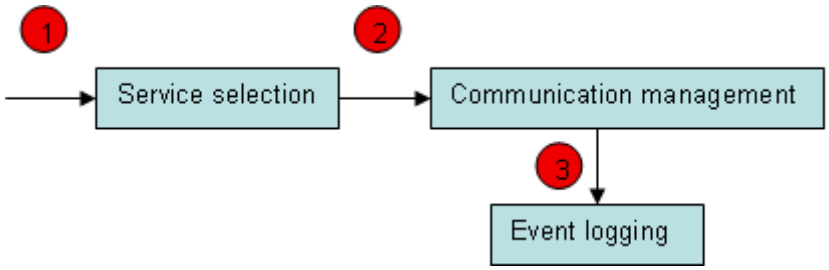


Figure 53 PUC 17: Multi-communication

A.11.3 Walk-through

A member, authenticated and authorised by the community, selects (via the Service selection {1}) the Communication management {2} in order to start the communication with other members. The Communication management manages the whole communication as well as the transfer of multimedia content. The Communication management closes the communication once it has been finished by all communication parties/members.

All actions performed are logged by the Event Logging component {3}

A.11.4 Reference to the User Scenario

Mark wants to share and discuss his new battle strategy with his allied players and provide them with the necessary information for the attack to be successful.

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

A.12 PUC 18: Organisation of ad-hoc meeting

A.12.1 Situation

A user/player uses the localization service in order to see if there are any other members of his/her (sub-) community nearby. He can see only those members who have appropriate privacy settings that allow other members from the same (sub-) community to see their current geo-location.

If the user finds somebody close to him, he sends an instant message to those users and invites them to the meeting. The invitation message delivery is based on privacy-related communication setting of each member of a given (sub-) community.

A.12.2 Reference diagram

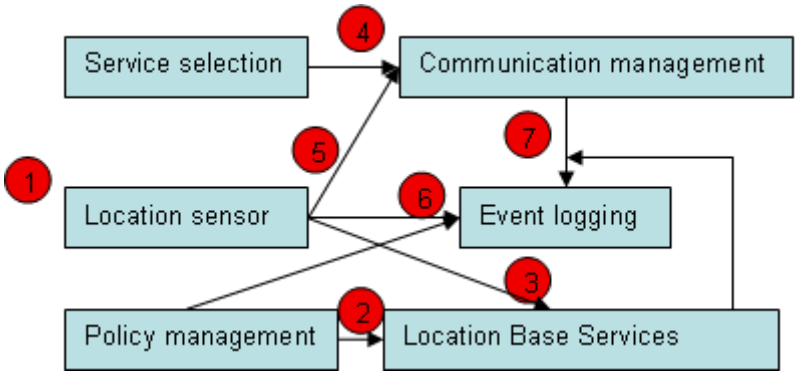


Figure 54 PUC 18: Organisation of ad-hoc meeting

A.12.3 Walk-through

A member, authenticated and authorised by the community, uses the Location sensor {1} to see his position. Based on his (and the members of his community) Policy management {2}, he uses the Location Base Services {3} to observe the position of the members of his community (those members must allow this setting in their Policy manager). After seeking the members of the community the user select the Communication management via the Service selection {4} in order to start the communication (in order to organize the ad-hoc meeting) with other members.

All actions performed are logged by the Event Logging component {6, 7}.

A.12.4 Reference to the User Scenario

Mark wants to organize a meeting to see his new friends and to share his experience with the game they play together.

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

A.13 PUC 19: Marketing/Advertising

A.13.1 Situation

An advertising service wants to attract gamers for gaming related products and services (virtual items, hardware equipment, etc.). Advertisements are placed based on a set of individual characteristics of players (target profile, e.g. age, hobbies, overall playing time (~ experience)) or average playing time per day/week/month. Advertisements are highly personalized based on these characteristics and based on the context of a user (e.g. location). Players receive a small hint at first, which indicates an advertisement. The advertisement screen further provides a possibility to forward an ad to contacts, which might be interested as well.

A.13.2 Reference diagram

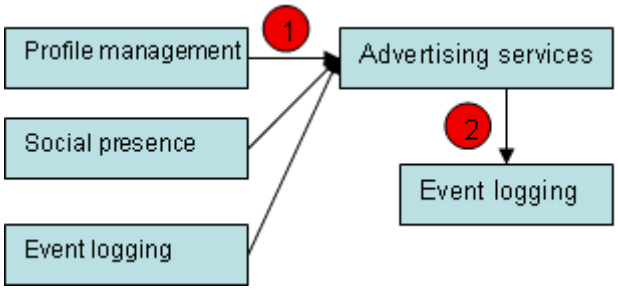


Figure 55 PUC 19: Marketing/Advertising

A.13.3 Walk-through

A member, authenticated and authorised by the community is shown an advertising/marketing message(s) based on his profile, social presence and past events {1}.

All actions performed are logged by the Event Logging component {2}.

A.13.4 Reference to the User Scenario

Advertising service wants to attract Mark to buy a brand-new mobile device with large touch-screen because he plays his favourite game(s) primarily on a mobile device.

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

A.14 PUC 20: Real-time content sharing

A.14.1 Situation

User wants to publish (persistently) new information about, e.g., future battle strategy (of his alliance) and planning in the game. The information should be visible only to other members of his alliance (if they have the appropriate access rights). The exchange of announcements, document, etc. regarding e.g., the strategy plan is carried out via the "Shared desk" feature. The other alliance members are informed if any of their members put some new content on this desk and are able to contribute own information.

The member who created and published the new information can set access rights/policies for other members of his alliance as who and (or even when) can access the published content. The member who created and published the new information can also check who has accessed the published content.

A.14.2 Reference diagram

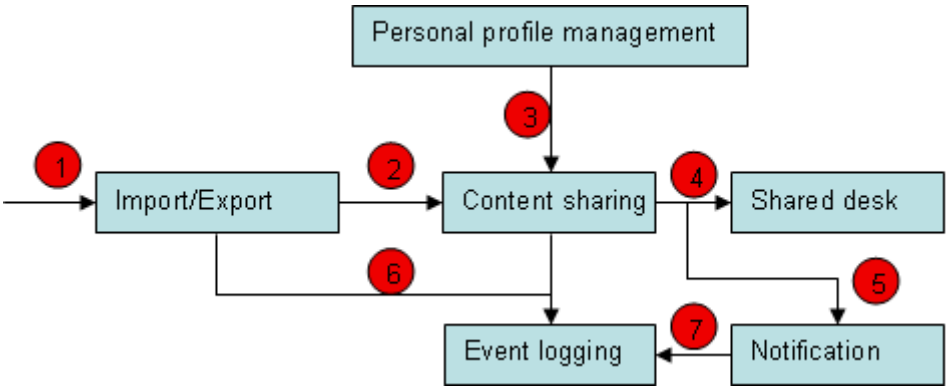


Figure 56 PUC 20: Real-time content sharing

A.14.3 Walk-through

A member, authenticated and authorised by the community, selects the Import/Export service and specifies the source of the content to be imported {1}. Next, the Content Sharing component tags the content {2}, taking tag information from the member and the member's profile {3} (and access restrictions if applied by the creator), and places the tagged content in the shared desk {4}.

Finally, the Content Sharing informs the Notification component to issue a notification that new content is available {5}. (Notification can be to the whole community, one or more sub-groups and/or specified members.)

All actions performed are logged by the Event Logging component {6, 7}.

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

A.14.4 Reference to the User Scenario

Mark wants to share newly created battle strategy with (all or a subset of) his allied players and provide them with the necessary information for the future attacks. He wants to be informed who saw the battle strategy even that this cannot serve as a proof that such member really read the instructions.

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

A.15 PUC 21: Enhanced social ads

A.15.1 Situation

An advertising service wants to attract gamers for gaming related products and services (virtual items, hardware equipment, etc.). Advertisements are placed based on the social and mobile context of players (e.g. current location, characteristics of current friends, location of friends, alliance memberships, playing experience, etc.). Advertisements are highly personalized based on these characteristics. Players are shown at to players which are in a similar social context (e.g. experience and current location). Players can give feedback on ads (like/dislike).

A.15.2 Reference diagram

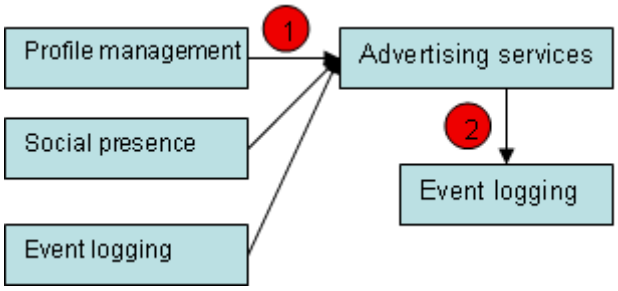


Figure 57 PUC 21: Enhanced social ads

A.15.3 Walk-through

A member, authenticated and authorised by the community is shown an advertising/marketing message(s) based on his profile, social presence and past events {1}.

All actions performed are logged by the Event Logging component {2}.

A.15.4 Reference to the User Scenario

Mark is in a city with his mobile devices and the location service is turned on. He gets an advertisement that there is a good restaurant nearby with free Wi-Fi access that he can use if he wishes.

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

A.16 PUC 22: Virtual marketplace

A.16.1 Situation

Players can offer game-specific items, or for example used/new mobile devices items they want to sell to other players. A player puts his/her offer to the virtual marketplace together with the item description, availability and required price. There is also a possibility to update the offer if the player wants to add some more information or, e.g., update the price of an item. Other players can browse through the list of offered items and contact the respective person for further details or for the selling instructions. Virtual marketplace does not offer payments and monetary transfers.

A.16.2 Reference diagram

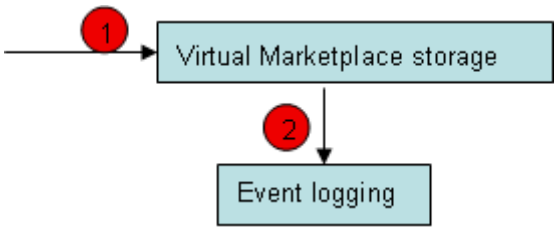


Figure 58 PUC 22: Virtual marketplace

A.16.3 Walk-through

A member, authenticated and authorised by the community can put his offer to the virtual marketplace or browse through existing offers and contact respective members in case of interest {1}.

All actions performed are logged by the Event Logging component {2}.

A.16.4 Reference to the User Scenario

Mark wants to offer his mobile device since he has just got a brand-new wide screen, hi-res PDA. He places his offer to the virtual marketplace, emphasizes the best features of his old mobile device and hopes to get a quick response.

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

A.17 PUC 23: Advertising Service

A.17.1 Situation

If a player visits an interesting place (e.g., free Wi-Fi access, good restaurant or bar) he/she can mark this place as a Point of Interest (POI) and store it for other members of his/her (sub-) community. POIs can be marked either "private" or "public" as required by the owner/player who created them.

A.17.2 Reference diagram

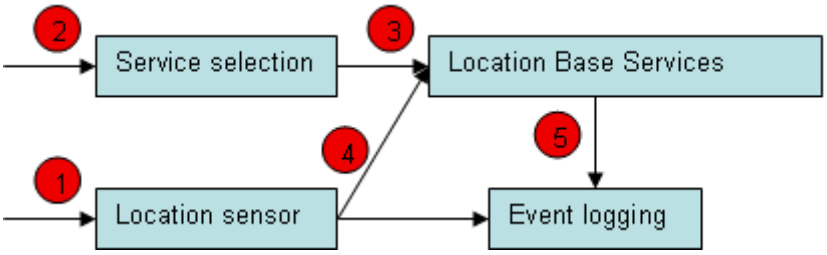


Figure 59 PUC 23: Marking a place as a Point of Interest (POI)

A.17.3 Walk-through

A member, authenticated and authorised by the community can use the Location sensor in order to retrieve the current geographical location {1}. This location can be stored as a point of interest (POI) by selecting the Location Base Services {2, 3}. The inputs are the geolocation and a description created by a member {4}.

All actions performed are logged by the Event Logging component {2}.

A.17.4 Reference to the User Scenario

Mark visited a good restaurant where he wants to meet with other players from his alliance, so he marks the place as POI and provides this information to players he wants to meet with.

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

Appendix B PICOS Principles

The PICOS Principles have remained unchanged since D4.1, although the descriptions provided here have been updated slightly to reflect our latest understanding.

B.1 PP1: Compliance with legislation

PP_{Law}

The PICOS Architecture must be compliant with all legislation, regulation and best practices that exist in the geographical regions in which the Community operates

As a minimum, information is handled and processed according to the EU Data Protection Directive.

B.1.1 Component contribution

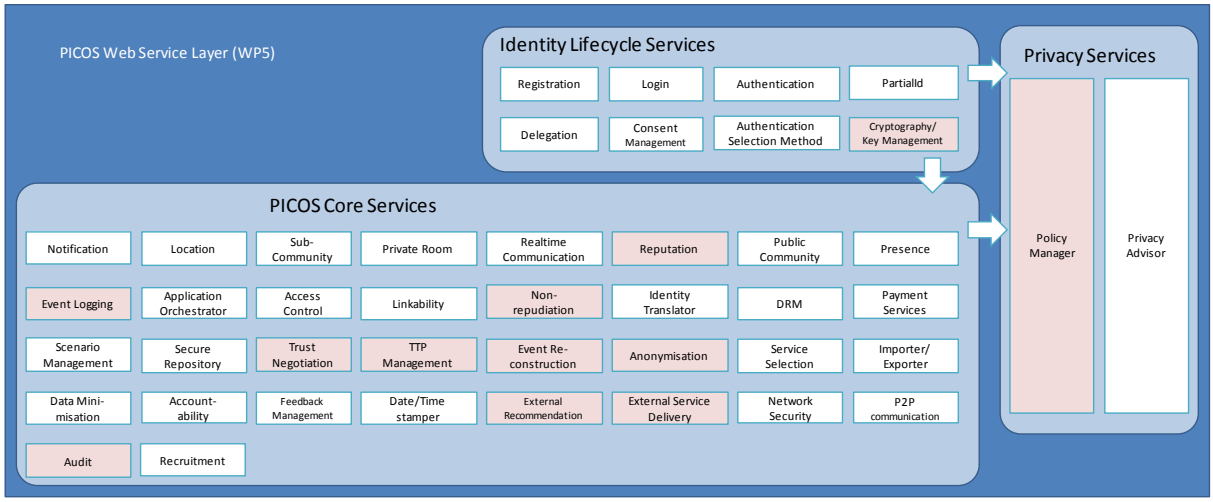


Figure 60 Components contributing to the PP Law

B.2 PP2: Data ownership

$PP_{Identity}$

The PICOS Architecture must recognise that personal information belongs to the Member that the information uniquely identifies

Members explicitly grant others, including the Community Manger (if one exists), the right to store and process their data according to the Member's stated privacy and data handling preferences. The PICOS Architecture ensures that processing is proportional to the stated purpose, and that the

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

Principle of data minimization is respected. For example, members may grant permission to the community operator to store and process their data according to the member's stated privacy and data handling preferences.

B.3 PP3: Use of personal information

PP$_{\text{Control}}$

The PICOS Architecture must provide members with the facility to state how their personal information can be used by others and, as far as is technically, legally and operationally possible, uphold the member's wishes regarding information flow and processing

Members state conditions that dictate how their personal information can be used by other Members. Conditions are enforced by the Architecture.

The degree to which control can be enforced is probably limited to within the community boundary, unless Digital Rights Management technology is deployed at the client or at third parties who are authorised to process member data.

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

B.4 PP4: Protection of personal information

PP$_{Control}$

The PICOS Architecture must at all times protect personal information to the level selected by the Member

Three classes of data are supported: non-personal data, personal data and sensitive-personal data. Personal data might include home address, telephone number, while personal-sensitive data include medical records.

The classification of each data item is decided by the owner of the data (typically the Member). Classification is subjective and difficult to define, but the approach just suggested (non-personal data, personal data and sensitive-personal) is in widespread use.

B.5 PP5: Openness and transparency

PP$_{Trust}$

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

Members will be more trusting if they fully understand the implication to their privacy of using services that handles their personal information.

B.5.1 Component contribution

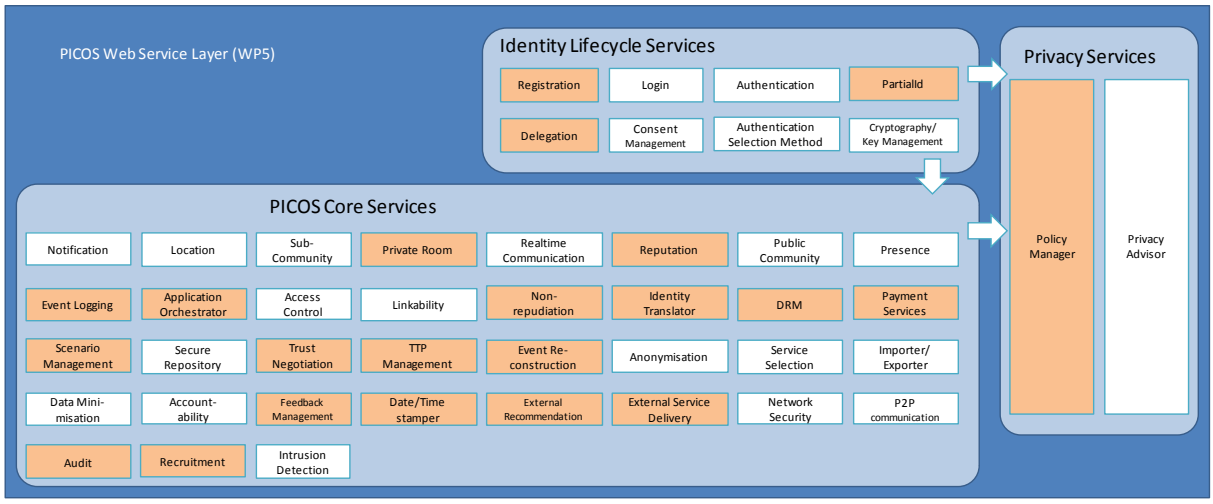


Figure 61 Components contributing to the PP Trust

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

B.6 PP6: Trust between communities

PP_{Trust}

The PICOS Architecture must recognise trust as a common currency when exchanged between PICOS communities

Members may belong to several PICOS communities. They will expect a seamless experience when interacting with Members across community boundaries, recognising that different communities focus on different 'themes', and different member's values, rules, behaviours. Portability of trust (or reputation) is highly desirable.

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

B.7 PP7: Topology agnostic

PP$_{Other}$

The PICOS Architecture should not be topology-specific

The Architecture is designed to be implemented on a range of interconnection (network) topologies, recognising that not all features are applicable in some configurations.

B.8 PP8: Data minimisation

PP$_{Privacy}$

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

While recognising that data minimisation is a principle adopted in European law, PICOS also appreciates that data is required in order to allow a community to grow. For example, Web 2.0 services are data-rich. A challenge for PICOS is to achieve an acceptable balance between these two demands. A solution may lie in the formation of trust, which allows greater use to be made of information in the knowledge that it is unlikely to be misused. Also, over time, we know from past research that trust itself grows, and community members are more comfortable sharing personal information.

B.9 PP9: End-to-end privacy

PP$_{Privacy}$

The PICOS Architecture must support end-to-end privacy

Where interacting Members are concerned that a central authority may be able to compromise (read/modify) their private interaction, the architecture should offer Members the option for end-to-end privacy (encryption?) subject to, and in compliance with, any legal obligations placed on the community operators (e.g. communication interceptions).

End-to-end privacy will not be required in all situations, and the trust that is placed in a community operator will be sufficient for most member needs (and reinforced by legislation). Also, providing end-to-end privacy makes law enforcement difficult or impossible, and therefore needs to be conditional.

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

B.10 PP10: Offline working

PP$_{Other}$

The PICOS Architecture must support online and offline working, and easy transfer between the two states

For a variety of reasons, Members may need to operate when disconnected from the Community, or be able to connect with a subset of the Community. Members will wish to be able to protect and process personal information belonging to them or to other Members when offline, and be assured the same level or protection as when connected (online) to the Community.

B.11 PP11: Use of pseudonyms

PP$_{Identity}$

The PICOS Architecture must present Members with the facility to be anonymous, to use pseudonymous identities or to use identities that are legally binding to that Member

Members will wish to interact with other Members and services, while still able to restrict how much identifying information is shared. They may vary the information shared for each interaction or vary it during an interaction. This is to allow Members to express their opinions with greater freedom, and to 'experiment' while they build confidence and trust in services and other Members. Note: While experimenting in isolation may be acceptable, using anonymising technologies when interacting with other Members may breach community operating practices.

Members may choose to be anonymous when providing feedback, or may have no choice if this is the default operating policy for the community. There are several possibilities. For example, reputation could be provided anonymously, but feedback intended to improve the community may identify the contributing member, and thus affect the contributing member's own reputation.

B.12 PP12: Provenance

PP$_{Trust}$

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

While it is probably too difficult to guarantee that information shared between Members is accurate, being able to rely on the source of the information is important for trust and reputation services. Note: This does not necessarily imply that the receiver of the information must be able to identify the originated, since the information alone may be trustable, e.g. because the source (not necessarily the sending member) is known and/or the content has been independently verified.

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

Where the source is not explicitly stated, the PICOS community may be able to give additional information about the level of trust (e.g. the reliability of the source, its profile or reputation rating.

B.13 PP13: External services

PP_{Trust}

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

Members may use services hosted by the Community to which they are currently connected, and Service provided by other PICOS communities. Ideally, all communities would operate at the same trust level, but in practice this is unlikely. Members should be able to determine from the nature of the Service, and not from a dependence on the hosting environment, how much trust to place in a Service.

Where it is hard to determine the trustworthiness of an external service, an indicator explaining to members that the service is provided externally may be sufficient.

For example, a contract (i.e. SLA) may certify that that the hosted service provider uses specific security technologies, trusted infrastructures, standardised procedures, etc.

B.14 PP14: Audit

PP_{Trust}

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

If something goes wrong, Members will expect to be able to recover and prevent a repeat of the event. Members will also expect accountability, both at Member and (if applicable) Community Operators level. There may be Legal or regulatory requirements to provide auditing for some community applications.

B.15 PP15: Data controllers

PP_{Law}

The PICOS Architecture must identify the controlling entity(ies) who are obliged to fulfil Legal obligations concerning the Community

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

For example, the Police may need to serve a Legal notice that obligates the Community to supply data about Members. Other entities will have similar statutory rights, e.g. the removal of copyright protected, illegal or defamatory information.

B.16 PP16: Objective and subjective trust

PP_{Trust}

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

Subjective methods include reputation management services. Objective methods include trusted computing bases and reputation management systems that are based on hard facts, e.g. system measurements, attributable actions and evidence of event fulfilment.

B.17 PP17: Authentication

$PP_{Privacy}$

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

Authentication should be possible using one, two and three factor (know/possess/are) methods. Health-related information must be adequately protected, treated as personal-sensitive information and respected according to the conditions stated by the Member.

B.18 PP18: Multiple persona

$PP_{Privacy}$

The PICOS Architecture should allow Members to have multiple persona

Members may want to operate within their PICOS Community, and between PICOS communities, under different identities (partial identities). One justification for this is to enhance privacy, for example by limiting linkability.

B.19 PP19: Sub-groups

$PP_{Privacy}$

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

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

If you take the Taxi Driver Community, the three taxi drivers operated independently of their drivers and (if included within the PICOS Community) their passengers.

B.20 PP20: Resilience

PP_{Other}

The PICOS Architecture must not have a single point of failure

For example, it should not have a centralised information store, single authentication point or single management function.

B.21 PP21: Diversity

PP_{Trust}

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

This does not relate to the general day-to-day management of the community, where placing the responsibility with a single entity does not represent a significant risk to the community, Member privacy or trust.

Keeping the community operational is something that a single entity could be responsible for, in line with the Service Level Agreement. Revealing anonymised members identities for law enforcement purposes might be something that requires the community operator to liaise with a TTP.

B.22 PP22: Trusted intermediary

PP_{Law}

The PICOS Architecture permits several trusted intermediaries (including external TTPs) to co-operate and link partial to real identities

This will almost certainly be required for legal purposes, and may be necessary for other purpose, e.g. to enhance reputation through external assurance or split responsibilities, and to provide non-repudiation services.

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

B.23 PP23: Trust

PP_{Trust}

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

All activities within the community are logged, and contributions are linkable to a real-world identity (by the community operator under a split role).

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

Appendix C PICOS Features

With the exception of the Web Front-end Extension, the core PICOS Features, which are described in this appendix, are as presented in D4.1.

C.1 PF1: Reputation

PICOS$_{\text{enhancing}}$

C.1.1 Description

Reputation covers rating and feedback. PICOS enables a community to keep track of user behaviour by computing a reputation indicator (typically a single value) for each individually identified member. This reputation indicator is produced for each pseudonyms generated under a member's real identity, and shared with other members without revealing the real identity in a way that might link pseudonyms.

In addition, a reputation component is able to aggregate reputation indicators from external communities and combine with 'local' community indicators, assuming that a meaningful association can be made. This process is initiated 'on demand', solicited by the requesting member.

Since different communities may express reputation in different ways, a process of normalization may be required. This process also 'weights' the reputation indicator associated to a given identity, and then aggregates the normalised values to obtain a single personal (i.e. subjective) reputation indicator. This computation will be performed without revealing any private information about the identities being evaluated.

When members provide feedback to other community members, or rate community-related activities, their reputation indicator will be linked, and consequently may affect how other members value their contribution. For example, a rating coming from a member with low reputation could have little credibility. In fact, members may choose to filter out certain contributions by setting a threshold that defines minimum (lower bound) reputation for them to be accepted. The same technique can be applied to items (as opposed to members) to assist when searching for information within the community.

Reputation indicators are influenced by the feedback that members provide, and based on personal experience. Thus, positive feedbacks will increase member reputation, while negative feedbacks will decrease it.

To ensure that the reputation system is reliable, only registered/authenticated members are permitted to provide input that influences reputation indicators. This is required to avoid the possibility that the reputation system becomes devalued by false, incorrect or malicious feedback. It is likely that other checks will be required that strongly associate members with the actions that they choose to comment on.

We talk about reputation indicators without precisely defining what form an indicator will take. This is because we want to allow for member to be able to customise the output to meet their particular

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

purpose and social values. Customisation will be achieved using the member's personal profile information where, for example, weights may be specified and applied to the reputation computation.

C.1.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Accepting and properly handling cross-community reputation, and whenever possibly valuing transitive trust indicators
- Ensure that feedback originates from an identifiable source
- Ensuring that feedback can be provided anonymously
- Demonstrating that the reputation system is trustworthy by building on open (transparent), robust design principles
- Within the community, creating a culture that encourage constructive feedback, and eliminating non-constructive influences

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

C.2 PF2: Content sharing

PICOS$_{enhancing}$ PICOS$_{mobility}$

C.2.1 Description

Content sharing comprises various activities concerned with the exchange of different types of information within a community (inter-community) and across communities (inter-community). Sharing involves several distinct phases that contribute to the exchange process, namely contribution, storage, administration, manipulation, communication (notification) and distribution of content. In practice, a specific mechanism would be required for each function.

Content is a general term that we use to refer to generic information, which may be represented as text, graphics (pictures), albums, videos and audio data, personal messages. It may also be encrypted, with decryption being possible at a system or an individual member level.

- Contribution: The process of making content available to other community members, involving mechanisms to perform the uploading of information (files).
- Administration: Administering previously contributed content within the community, including tasks for (re-)structuring and managing content. Administration also enables members to set privacy requirement on content contributed, thus they can control access to content by other members.
- Manipulation: Provides mechanisms for the manipulation of contributed content, including the partial editing of content, renaming, tagging, and deletion.
- Communication: Allows the mode of sharing to be specified, e.g. direct member to member, member to group of members and member to forum, and indirect exchange via a central repository using a push-pull procedure.

C.2.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Providing mechanisms for members to control how their content is shared with other, including compliance with any regulatory or legal constraints that may apply
- Allow content to be tagged in various ways, and for tags to be evaluated by other members
- Enable sharing to be controlled according to member attributes, including context (e.g. location) and recipient properties (e.g. reputation), including intra-community sharing
- Provide recommendation on the possible risks associated with sharing, by 1) taking into account preference, personal profile, the profile of recipients, context, the nature of the information being shared and 2) helping members identify (search for) other members who have similar interests and match the contributor's acceptable trust profile (where the trust profile includes a reputation threshold).

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

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

C.3 PF3: Registration

PICOS enhancing

C.3.1 Description

Registration is the first point of contact for individuals who wish to use a PICOS community. It is where information about the individual is collected, where roles and privileges (rights) are assigned, and where information associated with the authentication of the individual (subsequently known as member) is assembled (e.g. passwords, cryptographic keys). Registration encompasses authentication, identity management and de-registration. It represents the first step in the lifecycle management of community members.

Once membership is confirmed, members can create different identities (pseudonyms) so that they can represent themselves in different ways within the community. For example, a given member may choose a different pseudonym for a specific context, and with that context wish to operate under different privileges or profiles.

Members act under different pseudonyms to protect their privacy, possibly simultaneously. Pseudonyms are not linkable, and to all other member each pseudonym appears as a distinct, unique member. Reputation is based on unique identities (real or pseudonym), enabling other members to establish (track) specific contributions and related activities. For convenience, members may choose to share/transfer profiles/privileges between their identities, but PICOS will ensure that unlinkability is never compromised.

In addition to having real and pseudonymous identities, members can choose to act anonymously. Anonymous identities should not be confused with members' identities being anonymised by the community, for example when contributing feedback to the reputation component.

Membership of the community can be revoked at any time, for example:

- When a subscription expires,
- If the member freely decides to 'resign' membership,
- If the member behaves dishonestly or breaches to terms and conditions under which membership was accepted

C.3.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Offering an authentication mechanism that guarantees that members are who they say they are, and consequently have rights to the claimed privileges
- Establishing a sound, reliable identity to which reputation can be built.

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

- Through identity, supporting non-repudiation, which ensures that members are accountable for their actions, even if performed under a pseudonym.
- Protecting identity by allowing pseudonymous (and to a lesser extent anonymous) transactions, which when correlated do not allow disclosure of personal, identifying information. This is achieved while still building trust by tracking member activities as part of reputation management.

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

C.4 PF4: Personalisation

PICOS enhancing

C.4.1 Description

Every community member will possess a personal profile. The profile will be partly public and partly private. It will describe members' unique characteristics and their shared interests, but it will also provide members with an opportunity to state on what basis they are willing to interact with other members and generally make use of the community.

We understand from earlier (e.g. D2.4) deliverables and previous research (e.g. Trustguide[16]) that community members value choice and the ability to express personal preferences when interacting with others members within the community.

The profile is more than just a list of requirements. If forms the basis of the Privacy Advisor which is designed to help members to determine trust and maintain privacy in a way that is personal and unique, befitting their personal, continually changing requirements.

C.4.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Managing personal profiles by enabling members to create, modify and delete their personal profile
- Controlling visibility by enabling members to define exactly what information placed in the profile can be viewed by other members, groups, the community operator and external service providers.

[16] Trustguide. Final Report. Research carried out by HPL for the UN Government, investigating Trust in ICT. www.trustguide.org.uk

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

C.5 PF5: Messaging

PICOS enhancing

C.5.1 Description

Note: We use the term 'messaging' to refer to the exchange of information between an identifiable originator and recipient(s). We exclude what might be best described as broadcast systems, under which we including blogging, wikis and message boards. We accept that in a closed PICOS community, where membership is reliant on registration, and consequently everyone is identifiable, this constraint does not hold. However, we believe that where privacy is concerned there is an expectation that all parties in an exchange will already be known ('a posteriori') by name or personal characteristic to the originator.

Messaging is the exchange of information over a distributed and potentially unprotected medium, e.g. the Internet. We identify three distinct forms of relationships between members:

- One-to-one (1:1), e.g. via Instant Messaging (IM), private chat room
- One-to-Many (1:n), e.g. one member sends a message to which many members respond

The third case, which we exclude from the discussion on messaging, is:

- Many-to-Many (n:m), e.g. a public chat room where many members create messages simultaneously which receive many responses.

Originators of messages decide who can read, modify and/or forward their message to other members within the community. Originators remain the owner of messages sent, and can view records (logs) that show who has accessed a message, and can request to be notified automatically.

Logging of message is limited to message routing information only. Message content is not recorded unless specifically requested by the originator. Respondents to messages must be alerted to the fact that content logging is occurring before they reply.

Owners set access rights and apply other restriction, e.g. no print or local storage permitted. Special conditions may apply to messages sent to third parties.

To maintain privacy, message transmitted over unprotected medium are encrypted, thus preventing messages from being read or altered by anyone not authorised to do so.

C.5.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Encrypting information that passes over unprotected mediums
- Ensuring that recipients are identifiable to the satisfaction of the originator
- Observing originator preferences which may include reputation threshold requirements

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

- Logging events relating to message access and optionally logging content

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

C.6 PF6: Searching

PICOS enhancing

C.6.1 Description

Searching for information on the Internet is an exciting issue. It seems that there is nothing that users want that cannot be found, and there are billions of users who benefit everyday from the Internet. However, when searching in the entire Web, a specific website or an online community, users leave behind traces which allow their visit to be tracked. Their behaviour and interests can be observed, and potentially (mis)used by third parties. For example, simply browsing an online retailer can lead to the creation of a personal profile (interests, related products, etc.) which may result in users receiving unwanted advertising when they next visit the website, or unsolicited e-mails.

A quote from the New York Times reads, 'It may be easy to forget that there are people who want to remain anonymous on the Web while the online world is full of those who happily post pictures of themselves and their navels for all to see. But interest in software that allows people to send e-mail messages that cannot be traced to their source or to maintain anonymous blogs have quietly increased over the last few years, say experts who monitor Internet security and privacy.'[17]

Searching includes searching the community both for members and for content. It can relate to a specific, unique target or to targets that satisfy a set of conditions. It is an 'internal' service, that helps PICOS function, and it is a member service that supports many of the features that are offered to members.

C.6.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust while searching by:

- Protecting against traffic analysis: developing measures that allow individuals to share information over public networks without revealing their privacy.

Examples of techniques which PICOS could exploit include an adaptation of 'onion routing' (e.g. TOR), where users transactions are distributed across the Internet so that transactions cannot be easily linked to the member identity.

- Cookies management: HTTP cookies have been, and continue to be widely used when searching the Internet. They are used for authenticating, session tracking and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts. Cookies have brought personalization, commerce, and convenience to website browsing but have disadvantages which PICOS will address, e.g. unauthorised intercepting (cookie hijacking), unauthorised modification (cookie poisoning) during transfer between user and service provider; unauthorised cross-site 'cooking' (preventing a

[17] Citation from: "Privacy for People Who Don't Show Their Navels", by Jonathan D. Glater for the New York Times.

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

cookie for one website being transferred/used at another website) and providing user control over cookie expiration.

- Implementing, disposable, temporary identities which allow members to receive responses to search requests without needing to reveal their permanent or regularly used identity.
- Not breaching non-linkability rules

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

C.7 PF7: Sub-communities

PICOS$_{\text{enhancing}}$

C.7.1 Description

Functionality to create and manage sub-groups is one of the valued characteristics of community services and also one of the PICOS key features. Sub-groups allow easier communication and content sharing and form an important factor in the fine grained access control to data. Sub-community feature covers the creation and management sub-groups, e.g. buddy list, family & friends.

C.7.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Ensuring that only community member with appropriate rights can create, manage and delete sub-groups
- Ensuring that a community member with appropriate rights can remove unwanted members from a particular subgroup
- Supporting both global (e.g. projects, special interest groups) and personal subgroups (friends, family, etc.)
- Allowing Sub-groups to be categorised as open, restricted (membership by owner approval) and invitation-only. Selection can be made by member identifier or other characteristics, e.g. context or reputation
- Restricting visibility of sub-group membership to the owner and other members, as agreed with the specific member concerned. Such restrictions may form part of the member profile or preferences. Thus, membership may be visible to all members, only approved sub-group members or specified sub-group members.

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

C.8 PF8: Presence

PICOS$_{enhancing}$ PICOS$_{mobility}$

C.8.1 Description

PICOS defines Presence as a combination of online status and context information, e.g. location. Presence is tightly coupled to the communication services such as chat (Instant Messaging – IM) and indicates a member's availability for conversations with other members. Members can control both community-wide visibility or choose to restrict/permit visibility to specific members.

Presence can affect how trust and privacy is provided. For example:

- Privacy (more accurately referred to in this situation as confidentiality) is respected in many aspects of a presence system: Members may choose not to reveal to the community that they subscribe to certain services; Members may not want to reveal that they reveal their status to certain members; Members can conceal from others the information that they retrieve from information providing features like Presence.
- Confidentiality is provided through a combination of hop-by-hop (point-to-point) and end-to-end encryption. The hop-by-hop mechanisms provide scalable confidentiality services, disable attacks involving traffic analysis and hide all aspects of presence messages. However, since they typically operate on the transitivity of trust, they may cause message content to be accidentally revealed to proxies. The end-to-end mechanisms do not rely on transitivity of trust, and only reveal information to the desired recipient. However, end-to-end encryption cannot hide all information, and is susceptible to traffic analysis.
- Strong end-to-end authentication and encryption can be achieved using asymmetric (public key) cryptography, while end-to-end encryption is easier achieved with symmetric (secret key) cryptography. Hop-by-hop and end-to-end mechanisms are required to address privacy concerns that the Presence feature may give rise to. For example, the SIP protocol (used to access services offered by most mobile phone operators uses hop-by-hop encryption, whereas TLS (an end-to-end scheme) is the default (and often only) option on Web-like servers, leaving TLS as the obvious choice. An alternative is to encrypt SIP messages using S/MIME.

C.8.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Providing members with choice over who can see their Presence information
- Protecting information provided by the Presence service using strong encryption
- Strongly authenticating members (or their appliance) when requesting Presence information, thus the authentication may vary with presence (e.g. location).

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

C.9 PF9: External services

PICOS$_{enhancing}$ PICOS$_{mobility}$

C.9.1 Description

Communities benefit by the introduction of external services and resources, for example advertising, licensing, and traffic info. The overall functionality, from the member's perspective is enhanced and new application, use cases and business models can be supported, overall increasing the attractiveness of the community.

By providing information about members to advertising partners, in a privacy respecting way, members can receive information and offers that closely match their particular interests. This information can be integrated in existing or new services. For example, traffic information would greatly benefit one of the PICOS reference communities, namely Taxi Drivers, enabling them to optimise tours and find the quickest way to a destination or pick-up point.

PICOS will provide open, generic and flexible interfaces to external service providers, catering for both new and legacy features.

C.9.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Protecting member data delivered to external partners based on member privacy preferences profiles, and by not identifying members uniquely outside of the PICOS community
- Respecting the rights of members, as established in legislation (e.g. the EU Data Protection Directive) when personal information is shared with third parties
- Providing external services (especially advertising) to members on an opt-in basis, so that members can assess and decide on the added benefit that an external service may offer then
- Logging interactions (but excluding personal information) exchanged with external services
- Ensuring that external services are closely monitored and their operation is described to members in an open way so that members can make informed decisions on whether to subscribe to a service or use its features
- Handling complaints about external services without revealing more user data than necessary

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

C.10 PF10: Content tagging

PICOS distinguishing

C.10.1 Description

Content tagging covers the association of 'type indicators' (or tags) to information processed by the PICOS community membership. For example, tags might describe information that provides a location or that indicates that a member is mobile. Tags are semantic text elements, or meta-information, that describes content. They can be applied to a wide range of content including documents, video, audio and community operational information. They may be used in order to identify information received from external third parties, e.g. advertisers. They typically describe content in greater detail, and can relate to specific items, e.g. names of people in a photograph and the setting (e.g. 'summer holiday 2008'). The semantic nature of tags serves as a basis for a PICOS community to efficiently manage many different types of content the members may generate, e.g. organising, searching and making recommendations.

PICOS adopts three types of tag to ensure that members have adequate control over the content that they manage:

- Personal tagging: Only the member who contributed the content can tag the content
- Restricted tagging: Only members specified by the content contributor can tag the content
- Unrestricted tagging: All members of the community can tag to the content.

Mobility is an important feature of the PICOS community, so naturally tagging of location based information is regarded as highly desirable and important. Location based tags are tags that include information about the current location, e.g. 'geo' coordinates; location information and additional context information, e.g. time, place and mobile appliance, could be offered to members so that they can tag content in a way relevant to their mobile lifestyle.

Tagging also has a role to play in access control and in expressing context sensitive privacy preferences. For example, a member may tag personal health information so that any medical professional can access it, but only when the member is located abroad or away from their own regular Doctor.

C.10.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Using tags to restrict access to specific content that they contribute to the community
- Allowing members to decide how tags are applied and who can subsequently alter these tags.

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

C.11 PF11: Communication services

PICOS$_{enhancing}$ PICOS$_{mobility}$

C.11.1 Description

Communications services cover a wide range of member-to-member(s) real-time, video and audio (chat) services. PICOS assumes that mobile communities will (at least initially) make extensive use of mobile communication services, e.g. GSM. The integration of mobile communication services with a community service raises new privacy and trust issues, but also provides members with increased convenience when interacting with their community. For example, it will:

- Support anonymous communication, allowing members to interact using mobile communication services without exposing mobile phone numbers or other identifiers, e.g. by replacing a Caller ID with a member identifier (possibly pseudonymous, and ensuring that no personal identifying information is revealed in received call / missed call lists, or detailed in billing records, etc.
- Enforce privacy policies when sharing member-generated content within multi-media communication sessions. For example, a pre-defined set of members who are permitted to access/view photographs or video clips, would still apply when those same images are present over a mobile communication channel.
- Enforce member policies with regard to reachability, i.e. control how a member can be contacted when they are using specific communications mechanisms (messaging, voice, video), and when other constraints apply, context, location, 'buddy lists'.
- Provide privacy-aware caching of community information at the mobile device. Information might include contact information, and additional restrictions may apply after transfer, e.g. allow download but prevent subsequent forwarding to other members.
- Support "anonymous" communication, where members can communicate peer-to-peer using their community member identifiers (i.e. without disclosing phone numbers or other identifiers)
- Enforce privacy preferences, which are applied before sharing member-generated content over a real-time communication services

Ideally PICOS will embed (integrate directly into the PICOS architecture) most communications services, some may be offered by a third-party providers, e.g. a mobile operator. Tight integration is preferred because it means that all communication is triggered from within the community and consequently privacy policies can be instantly applied. Communication that takes place outside of the scope of the community platform raises questions about how policies can be applied and tightly coupled to content.

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

C.11.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Respecting privacy preference and content tags regardless on the communications service offered, or of the form in which the content is presented to the member
- Anonymising personal information that would otherwise reveal the identity of those engaged in the communication.
- Controlling the application of content communicated to members by enforcing preferences applied by the originator, e.g. read but no onward sharing.

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

C.12 PF12: Notification

PICOS$_{enhancing}$ PICOS$_{mobility}$

C.12.1 Description

Previous deliverables (e.g. D2.3, D2.4) and other research (e.g. Trustguide) revealed that members are more likely to trust a community when they understand how services operate. Describing how personal content is processed, in an open and transparent manner, engenders trust. Thus, keeping members informed about the status of the community, their outstanding transactions or other information that relates to their personal use of the community, through the use of notifications and alerts increases confidence.

C.12.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Reporting status information covering:
  - System and service delivery status
  - Community status
  - Member status
  - Inter-community status
  - Activity status
- Enhancing decision making by providing information covering:
  - Context-based, risk indicators
  - Past performance derived form historic status information
  - Alignment with personal profile
  - Previous actions/decisions
- Offering advisory information covering:
  - Events arising from real-time status information
  - Significant changes in community structure
  - Member activity
  - Deviation from personal profile

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

C.13 PF13: Intra-community interaction

PICOS enhancing

C.13.1 Description

The aim of this feature is to allow identities created in one community to be used in several other linked communities, while maintaining a coherent level of privacy and security. Inter-linking of communities may imply non-trivial organizational and implementation issues and will require a certain level of trust among the inter-linked communities.

Other attributes can be similarly transferred across community boundaries, including privileges and reputation information, such that the identities in each community refer to the same real individual. This forms part of the federated identity management feature of PICOS, where members of one community may have automatic right to access another community based on their reputation. In such a case, registration is not required, except with the first community a member joins, and privileges are transferred automatically to any additional community. An example can cover situations where an angler based in Germany wants to access resources from an angling community in France without the need to first register on the French system.

C.13.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Only interacting with neighbouring communities if the Administrators of both communities agree on the inter-community linking
- Setting security level for all connected communities that meet certain minimal requirements, e.g. standard for the encryption of transmitted passwords, the level of security applied to servers
- Ensuring that the identity of a member can be used in other communities only if the user has expressed consent with such an identity sharing
- Allowing each member to choose whether they wish to explicitly approve each additional community linked to, or letting members configure their personal profile to automatically include all inter-linked communities (or some specific groups based e.g. on subject, location).
- Mutually respecting access restriction imposed by member of neighbouring communities
- Ensuring that exchanged content can only be used as instructed by the contributor
- Not linking a member to any community that they have expressly asked not to be connected to.

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

C.14 PF14: Mobility

PICOS$_{distinguishing}$ PICOS$_{mobility}$

C.14.1 Description

PICOS supports mobility. Mobile devices present new challenges to an otherwise static community: different technologies and additional use cases.

The different technologies comprise the communication network and the devices. The network uses different methods to transport data (not always transparent to the application and user) and provides additional services including short messaging, network-based authentication, and location and presence services. Also, the devices are adapted for mobile use and typically have reduced size, limited usability, reduced power and less storage.

Mobility enables new use cases. Members now have access to the communities at any time and at any location. They might be using different devices for mobile and static access, and consequently want to synchronise the data held by their two appliances. Based on additional member data, e.g. current location, new services can be linked existing use cases offering enhanced features for the member.

C.14.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Securing connections over which messages pass between members
- Offering strong user authentication based on network attributes or temporary credentials
- Identity management and the inter-working of mobile devices and stationary devices
- Making full use of additional context attributes, e.g. location, presence, device capabilities
- Adapting the way that information is presented to members when using mobile devices to enhance usability.
- Responding to threats that are specific to mobile situations
- Controlling information flow between members via the PICOS community, to maximise member privacy

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

C.15 PF15: Non-repudiation

PICOSdistinguishing

C.15.1 Description

PICOS offers the capability to ensure that actions performed by members cannot be later disputed (repudiated). This is achieved by using digital signatures. Every contribution made by a member is digitally signed by a public key that is either directly or indirectly bound to the member's real identity. If a member contributes content using their pseudonymous or anonymous identity, then a continuous non-repudiated chain can only be constructed with the cooperation of one or more trusted third parties (TTPs), who together may be able to collude to compromise a member's anonymous or pseudonymous identity.

Note that non-repudiation can only be guaranteed if members individually control their private cryptographic key. It is crucial that any implementation provides sufficient protection to guarantee this requirement. Equally, it is important that bindings are not compromised registering unlinkable pseudonyms or performing anonymous actions.

If non-repudiation as provided supports a legislative obligation, then it is important that members are registered with the community using an externally provided non-repudiated mechanism, such as X.509 strong authentication and X.509 Public Key Certificates issued by a legal Certification Authority (CA).

C.15.2 How PICOS will address the privacy/trust/IdM concerns

PICOS will maintain privacy and build trust by:

- Enhancing member confidence by ensuring that member cannot repudiate contribution specific content.
- Ensuring that pseudonyms and anonymous identities cannot be compromised through weaknesses in the binding mechanism introduced by the non-repudiation mechanism.

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

Appendix D Dumb terminal architecture

This topology is based on the thin client model. Here, a 'dumb terminal' (web services portal) is used to access the community. This could be a smart phone that runs a simple client application that provides access (only) to the community, e.g. a browser. Apart for the access application, no other services are hosted on the client appliance; everything else, including My Services, is hosted centrally.

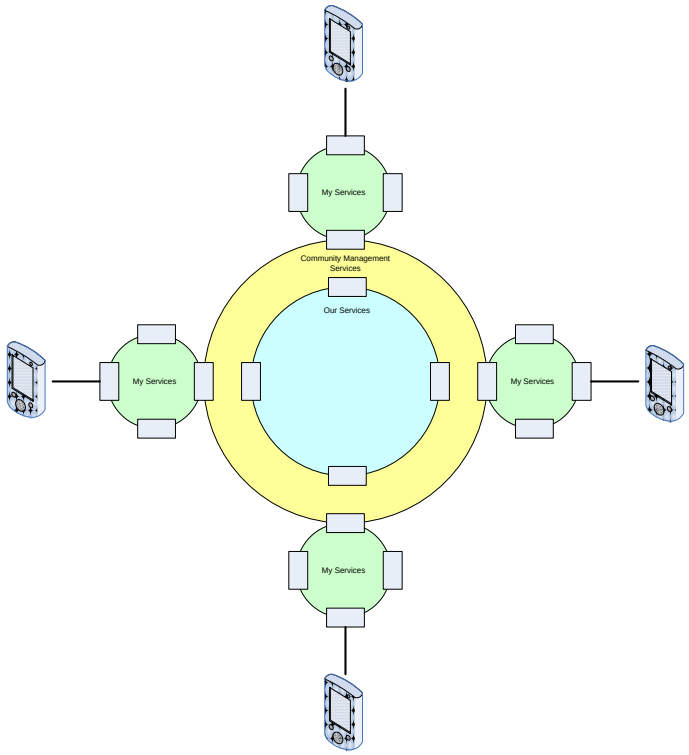


Figure 62 Dumb terminal topology

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

Appendix E Component descriptions

In this appendix, components that are either new or significantly enhanced since D4.1 are marked thus:

PICOS D4.2 new/updated component

The list on new/enhance components includes:

- Active Chat
- Advertising Services
- Alarms
- Contacts Management
- Location Based Services
- Policy Management
- Privacy Advisor
- Public Community
- Secure Repository
- Share Desk
- Sub-community Management
- User Availability Calendar

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

E.1 Communication Management

T_1

PICOS Principle (PP): 1, 4, 7, 10, 20

PICOS Feature (PF): 11

E.1.1 Purpose

The *Communication Management* component is responsible for providing and co-ordinating communication between members and the PICOS community.

E.1.2 Description

The *Communication Management* component provides a level of abstraction above other specific communication technologies. Whenever members or external services (service providers) need to communicate with the community, this component chooses the most appropriate set of mechanisms to establish the communication. This component is also responsible for managing the security of the communication, which is achieved by calling on the services of the *Network Security* component.

Example 1: An incoming communication is requested by a member via the *Service Selection* component. The *Communication Management* component detects the request and activates the appropriate communication medium, e.g. GSM, Wi-Fi, Bluetooth. The type of network security available may vary depending on the medium chosen, thus several steps may be required to establish a secure channel (encryption algorithm negotiation, key sharing, authentication, etc.). The *Communication Management* component is responsible for handling this detail, and will be expected to do so in a way that is transparent to other services.

Example 2: A member wishes to communicate directly with another member (P2). The *Communications Management* component will receive the request, and then established a secure channel using the *P2P Communication* component. As in Example 1, security will be achieved using the *Network Security* component under the direction of the *Communication Management* component.

A need may also arise to provide anonymous network connectivity, in which case the *Communication Management* component will call on the services of the *Anonymisation* component to support (for example) a TOR protocol.

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

E.1.3 Dependencies

Components that this component calls	Purpose
Anonymisation	To support use of a TOR protocol.
Network Security	To establish a secure, authenticated channel.
P2P Communication	To enable P2P communication between members

Components that call this component	Purpose
Service Selection	When requested by a member of another entity to establish a communication channel with another member or entity.

E.1.4 Drawing

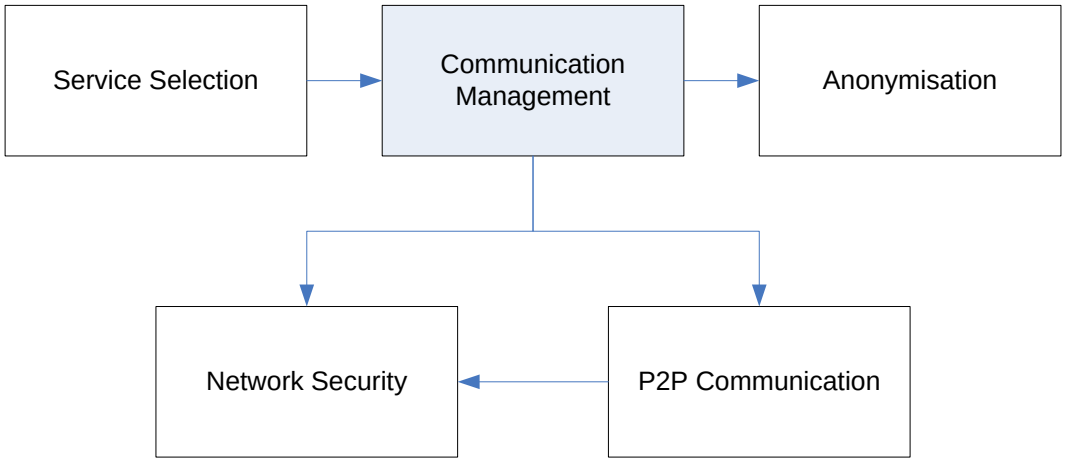


Figure 63 Communication Management component

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

E.2 Network Security

T_2 PICOS$_{enhancing}$

PICOS Principle (PP): 1, 4, 7, 9, 10, 11, 13, 20

PICOS Feature (PF): 11

E.2.1 Purpose

The *Network Security* component is responsible for creating a secure channel between communicating entities. Security includes authenticating end points, choosing appropriate security mechanisms and handling support functions, e.g. key management.

E.2.2 Description

The common interpretation of network security is the execution and control of mechanisms designed to protect the confidentiality and integrity of information that passes over a communication network.

Security can be achieved using the application oriented layers of the ISO OSI reference model (i.e. layers 4 to 7) in a supporting protocol like TLS (layer 4) or S-HTTP (layer 5). Alternatively, security in the form of transmission security can be realised on the network layer (layer 3 of reference model) over an IPSec protocol.

The aim of network security is to ensure that messages in transmission cannot be read or altered without authorisation, e.g. by a third party or an adversary. The strength of protection is sufficient to deter the most determined adversary.

In addition to confidentiality and integrity of data, network security can also provide authentication of communicating parties and authenticity of data. Privacy is an increasing issue which network security can address, by obscuring identities (originator/recipient identities). Network security can also offer end-to-end confidentiality using encryption.

Network security is typically initiated by the originator of the communication, in relation to the intended target. The originator can be a member using a client device, or it can be a centralised service that wishes to communicate with another service, another community or an individual member. In addition, communication may be directly between members, who may involve peer-to-peer (P2P) network security, or perhaps more realistically, with current network topologies, a secure communication channel orchestrated by a centralised service (the spoke-and-hub communication model).

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

In a mobile scenario, where a secure authenticated channel is required between client and server, TLS is a possible though not necessarily efficient option[18], providing member-to-member (pseudo P2P) protection.

The role of the *Network Security* component, which in practice may be distributed at several 'control points', is to implement the mechanisms that provide confidentiality, integrity and authentication at the data transfer layer. For key management and other cryptographic services, the *Network Security* component will call on the services of the *Cryptography / Key Management* component. The role of the *Network Security* component may be extended to anonymisation where, with the help of the *Anonymisation* component, originator/recipient identities can be obscured. An example of how this can be achieved is the TOR[19] anonymisation technique.

A further function of the *Network Security* component concerns traffic analysis. While encryption protects the content of a message, routing and other message characteristics can reveal sensitive information. Where possible, the *Network Security* component will ensure that no information leakage is possible.

[18] TLS has the problem that compression is inefficient, which may be an important disadvantage for the mobile scenario

[19] TOR is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet

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

E.2.3 Dependencies

Components that this component calls	Purpose
Cryptography / Key Management	For cryptographic mechanism and key management services in support of the request to secure a communication channel.

Components that call this component	Purpose
Communication Management	When setting up a communication channel that requires network security.
P2P Communication	When setting up a P2P communication channel that requires network security.

E.2.4 Drawing

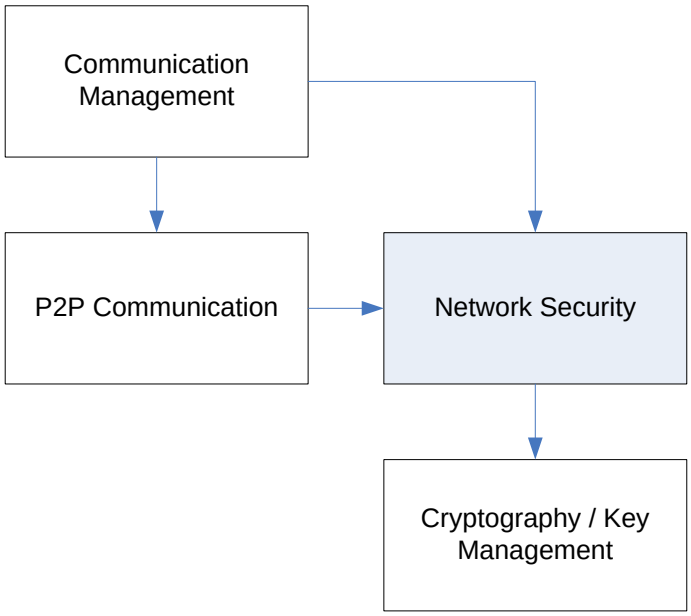


Figure 64 Network Security

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

E.3 P2P Communication

T2 PICOSenhancing

PICOS Principle (PP): 1, 4, 7, 9, 10, 11, 13, 20

PICOS Feature (PF): 11

E.3.1 Purpose

The P2P Communication component is responsible for establishing a secure channel between two peer entities, typically two members. The objective is to provide communication when no centralised service is available (e.g. a remote location where there is no mobile network coverage) or to isolate the content of the communication from the community (members and community operator).

E.3.2 Description

There are basically two kinds of communication that a PICOS community might support

- between a member and a service provider (client-server (CS), or Hub-and-Spokes)
- between peers, usually members (peer-to-peer, or P2P).

The P2P topology is mainly used in offline situations where no centralised connection infrastructure is available. P2P communication helps to overcome the lack of network coverage in a mobile setting. When connection to the server is re-established, the users are synchronized again with the server. In addition, P2P communication can ease the setup of ad hoc communities. Two members can initiate a communication between their mobile devices, e.g. by using Bluetooth.

The P2P component is responsible for the setup and release of direct connections, and for the transfer of data between members. It may also have a role to play in the subsequent synchronization of off-line data with centralised resources. However, it must be recognised that one reason for using P2P (as opposed to centralised communication) is privacy, thus data shared between members should not consciously be exposed to the community. This includes routing and other message identifying information.

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

E.3.3 Dependencies

Components that this component calls	Purpose
Network Security	To establish a secure channel

Components that call this component	Purpose
Communication Management	In response to a request for an entity (member) for a direct P2P secure connection with another entity.

E.3.4 Drawing

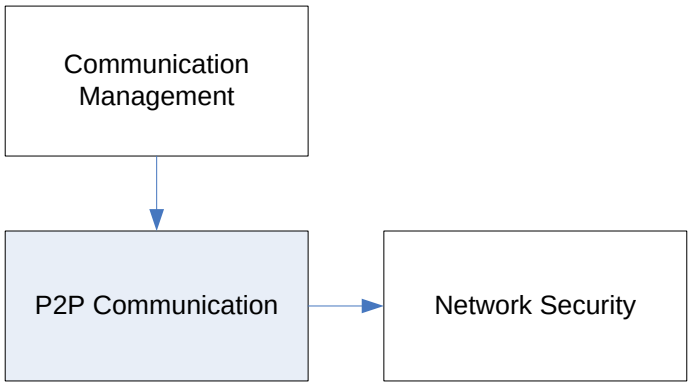


Figure 65 P2P Communication

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

E.4 Access control

T_1

PICOS Principle (PP): 3, 17

PICOS Feature (PF): 3

E.4.1 Purpose

The *Access Control* component responds to a request for access to the community. Typically this will be from a member, but could also be for an external entity, e.g. a service provider.

E.4.2 Description

The Access Control component appears as the first point of contact for visitors to the community.

This component acts as the gatekeeper, controlling access to all community resources. It combines authentication and authorisation functionality, which are both provided as separate Tier-2 components. The *Access Control* component also handles Guest and Third Party access, and co-ordinates access from entities that claim membership of a community that has a mutual relationship with accessed community (federated access).

On receipt of a request to access the community, the *Access Control* component gathers identification and authentication information which is passed to the Authentication component for validation. If authentication is successful, the *Access Control* component forwards the access request to the *Authorisation* component where the level of access permitted is determined.

Access requests may also be received for entities other than member, or from members of other communities. In such cases, the access request is processed within the Access Control component.

For new (prospective) members, the *Access Control* component co-ordinates the registration process by directing the request to the *Registration* component.

Guest members are not required to register or be authenticated, but receive significantly reduced community functionality. Guests are processed by the Access Control component and passed directly to the Authorisation component, where limited authority is granted.

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

E.4.3 Dependencies

Components that this component calls	Purpose
Authentication	To validate the identity of a member (entity).
Authorisation	To assign access rights to the member (entity).

Components that call this component	Purpose
Communication Management	To apply access control to an incoming entity (member).

E.4.4 Drawing

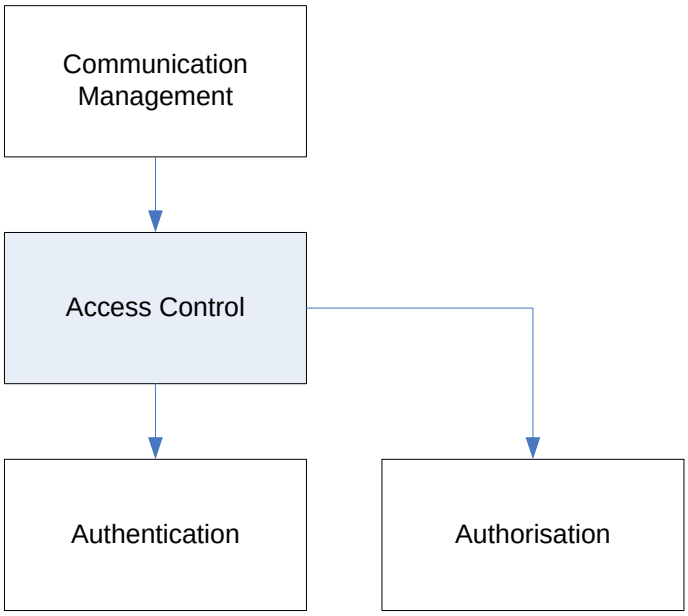


Figure 66 Access Control

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

E.5 Anonymisation

T2 PICOSdistinguishing

PICOS Principle (PP): 1, 4, 8, 11

PICOS Feature (PF): 2, 5, 9, 13

E.5.1 Purpose

The *Anonymisation* component is mainly responsible for creating pseudonyms (anonymous credentials), and may have a role to play in providing or co-ordinating anonymous communication (e.g. TOR anonymous networking technique).

E.5.2 Description

The *Anonymisation* component provides anonymisation functionality at the application and network layers.

Application layer:

Anonymisation at the application layer allows members to create and register new pseudonyms, which can be used as partial identities. Thus, the *Partial Identity Management* component relies on the *Anonymisation* component. (Each partial identity appears to the community as a unique member with unique privileges and reputation.) Members can use pseudonyms to interact anonymously with the community, as well as to access external services anonymously.

In the situation where a member (client) operates independently of the community, the *Anonymisation* component provides members with private cryptographic keys so that they can be authenticated as the rightful holder of a pseudonym or anonymised privilege. Keys are generated by the *Cryptographic / Key Management* component.

Also at the application layer, the Anonymisation component is involved in anonymising (or pseudonymising) data that exists after a member has resigned from the community. This process is triggered by the *Revocation* component. After a period defined by community policy (see Policy component), identifying information associated with data left behind by the resigning member is first pseudonymised in a reversible way (e.g. encryption), and later in an irreversible way (e.g. hash) such that personal identifying references are totally erased.

Network layer:

The *Anonymisation* component also anonymises Internet communication endpoints (i.e. the IP address of the initiator of a transaction). The component is called when a member wishes to interact anonymously/pseudonymously, and is most likely to be used when interacting with external service providers. Anonymisation at the network layer prevents correlation between transactions and IP addresses, which could be linked to a member's identity.

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

This facility is not always necessary, and its usage is optional dependent on context and member preferences. By way of an example, TOR (a second generation onion routing platform) provides this facility, but requires an external TOR onion routing network and a TOR-component client.

E.5.3 Dependencies

Components that this component calls	Purpose
Cryptography / Key Management	To create an endorsed pseudonym.

Components that call this component	Purpose
Communication Management	To request assistance setting up network level anonymisation, e.g. a TOR solution.
Partial Identity Management	To request an endorsed pseudonym.
Revocation	To anonymise data belonging to a departing member, according to the policy of the community (Policy Management component).

E.5.4 Drawing

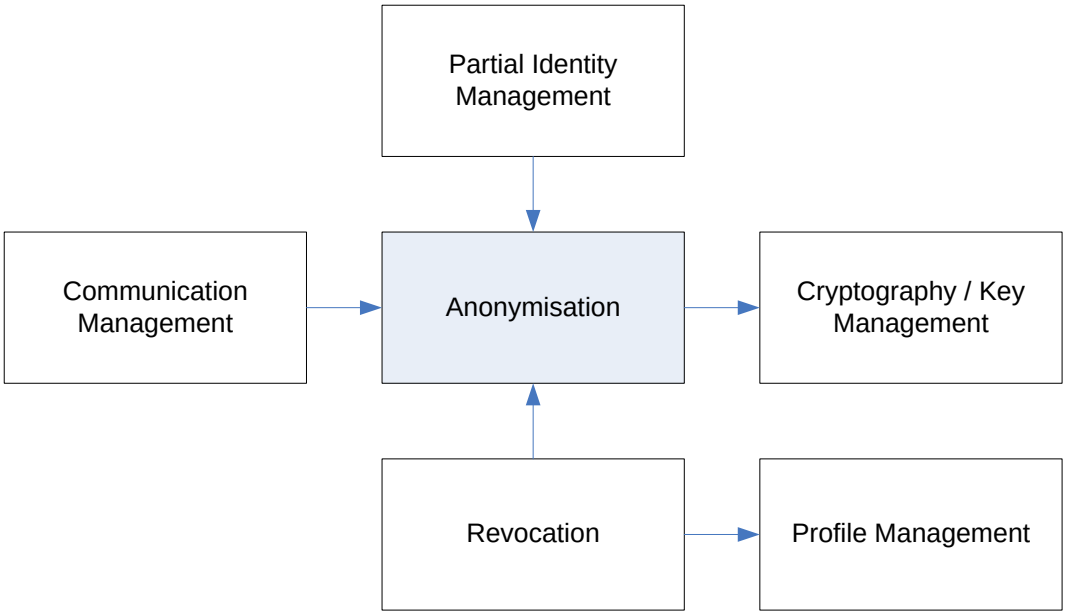


Figure 67 Anonymisation

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

E.6 Application Orchestrator

T1 PICOSdistinguishing

PICOS Principle (PP): 13

PICOS Feature (PF): 9, 13

E.6.1 Purpose

The *Application Orchestrator* component combines internal and external services to provide a richer set of functionality for members.

E.6.2 Description

Flexible services can help a community create privacy-respecting mash-ups (workflows) that combine information services and communication services, and content. This aggregation of services must be transparent to members. Aggregation allows the building of composite services by combining existing elementary or complex services available as part of the PICOS Toolbox or offered by external third parties. It achieves this by interacting with the External Service Delivery component.

For example, the taxi driver community describes a scenario where when picking up their child from school, parents would be happier if they could track the taxi in real-time and see an audit trail that confirms that the driver and child were in close contact at the prescribed time. Knowing that information about regular school pick-ups is protected, and being able to obtain reputation information about the driver on demand, would engender trust. In the angling community, a similar example might involve the aggregation of location, weather, a fish database and individual angling skills, to create a service that automatically plans a weekend fishing expedition.

The *Application Orchestrator* component serves two purposes:

- It provides a level of abstraction which presents aggregated services as single services, but hiding the implementation detail that is sometimes visible when interacting with multiply independent services. For example, services that may be provided as part of the PICOS Toolbox can be combined to create a richer set of functionality, while not exposing members to the fact that several services are involved. In time, this can lead to open standards.
- In a similar way, the orchestrating service provides a useful higher level of abstraction that benefits developers. Customising a community is simplified and bringing new services to members is quicker. Specific privacy preserving and trust enhancing features can easily be introduced, possibly in response to member requests provided by way of the feedback service. Greater flexibility would allow the developer to experiment and produce prototypes with ease.

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

E.6.3 Dependencies

Components that this component calls	Purpose
External Service Delivery	To access individual services.

Components that call this component	Purpose
Service Selection	To compose a set of services in response to a member request.

E.6.4 Drawing

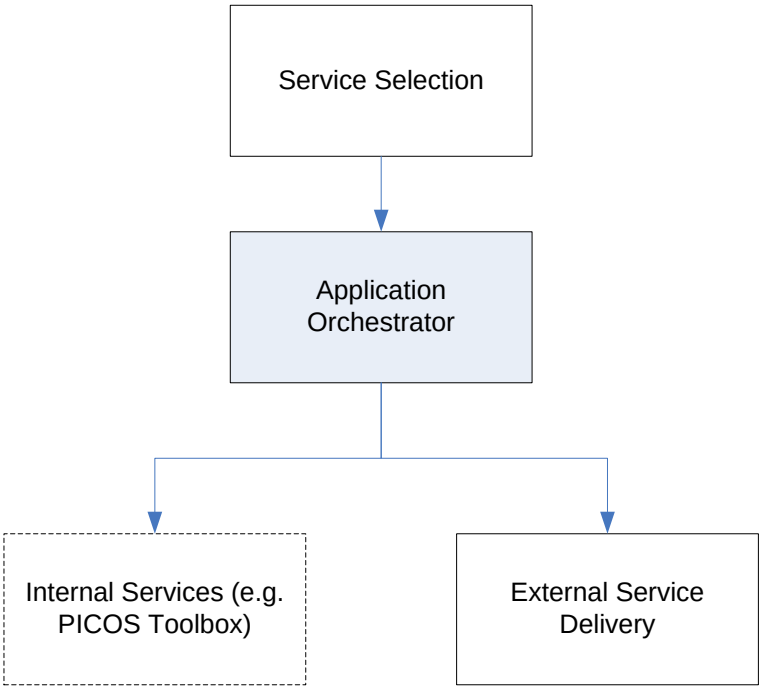


Figure 68 Application Orchestrator

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

E.7 Authentication

T2 | PICOSenhancing | PICOSdistinguishing

PICOS Principle (PP): 3, 17

PICOS Feature (PF): 3

E.7.1 Purpose

The *Authentication* component forms part of the access control process, and operates under the supervision of the *Access Control* component. The role of the *Authentication* component is to validate the information that a member provides when accessing the community and thus 'proves that they are who they say they are'.

E.7.2 Description

The *Authentication* component supports the community gatekeeper role, controlling access to all community resources.

All members are identified and authenticated before being granted access to the community. Identity is based of a previously registered partial identity. Authentication can be by credential, which includes an externally endorsed pseudonymous, personal identity token, platform identity biometric or traditional password. The means of authentication is set by the *Authentication Method Selection* component with respect to community Policy (determined by the *Policy* component). The *Authentication* component is supported by the *Cryptographic / Key Management* and *Secure Repository* components

After being authenticated, members are authorised to access the service to which they are entitled according to their membership privileges. Authorisation is determined by the *Authorisation* component.

Authentication information is protected during transmission between the member (client platform) and the community using an appropriate security/encryption protocol, e.g. TLS in the case of a mobile client.

Guest members are not authenticated, but only have access to a very restricted set of community services.

Third Party access, e.g. by an external service provider, would be subject to authentication unless other security checks are in place, e.g. access via a trusted channel or if subsequent checks are made on the authenticity of content submitted and shared with members.

The services of a TTP (CA) may be required in order to authenticate federated identities, accessed via the *TTP Management* component.

A useful description of how authentication is employed in PICOS can be found in sub-Section 13 in:

- PICOS Use Case 2: Accessing the community

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

E.7.3 Dependencies

Components that this component calls	Purpose
Authentication Method Selection	To determine the set of acceptable means of authentication for the member, according to community policy (*Policy Management* component). Authentication may require the co-operation of a Trusted Third Party (TTP), e.g. where registration took place in another community (*TTP Management* component.)
Cryptography / Key Management	To support cryptographic authentication protocols.
Secure Repository	To retrieve sensitive authentication information.

Components that call this component	Purpose
Access Control	To verify the identity presented by the member. Note: The *Access Control* component subsequently calls the *Authorisation* component

E.7.4 Drawing

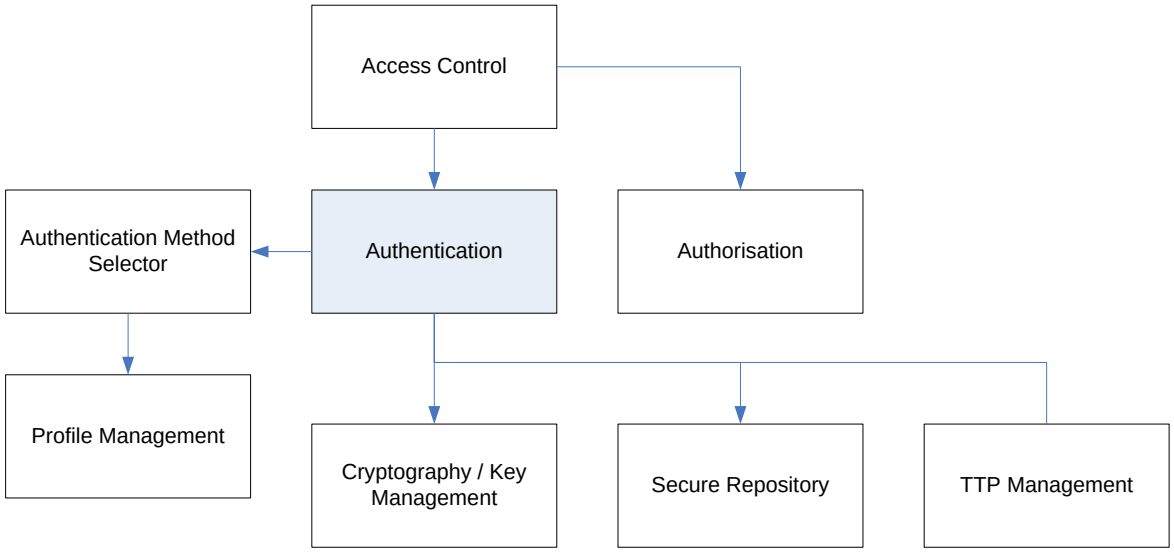


Figure 69 Authentication

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

E.8 Authorisation

T2 | PICOSenhancing | PICOSdistinguishing

PICOS Principle (PP): 3, 17

PICOS Feature (PF): 3

E.8.1 Purpose

The *Authorisation* component is responsible for assigning authenticated members the rights they have been granted.

E.8.2 Description

Members (and other entities) are authorised to access community services, subject to the following:

- Satisfying authentication requirements
- Being permitted by their profile to access the service
- Being permitted by their social presence (e.g. location) to access the service
- Receiving the consent of the service provider (particularly relevant in the case of an external service provider) or the content provider (in the case of requesting access to content provided by another entity.

The *Authorisation* component checks all of the above and, if the criteria are met, the member is allowed to proceed to the *Service Selection* component and presented with a set of available services as befits their role.

The *Authorisation* component is called whenever a member requests a service that has restricted access. For example, a member may be restricted for accessing a service for certain locations. Having accessed the community and received authorisation to import content, this privilege may subsequently be revoked if the member moves to another location (e.g. relocating from a work place to a public place). In such a case the *Service Selection* component might call the *Authentication* component before granting access to the service. A similar situation exists with reputation, which is another dynamic member attribute.

A useful description of how authorisation is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 1: Registration
- PICOS Use Case 2: Accessing the community
- PICOS Use Case 4: Multiple Partial Identities

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

E.8.3 Dependencies

Components that this component calls	Purpose
Profile Management	To retrieve privileges assigned to the member.
Social Presence	To check current status of the member

Components that call this component	Purpose
Access Control	As part of the access control process governing access by members to the community. Note: Authorisation is called after calling the *Authentication* component.
Service Selection	When a member requests a service that is only available depending on current (real-time) social presence.

E.8.4 Drawing

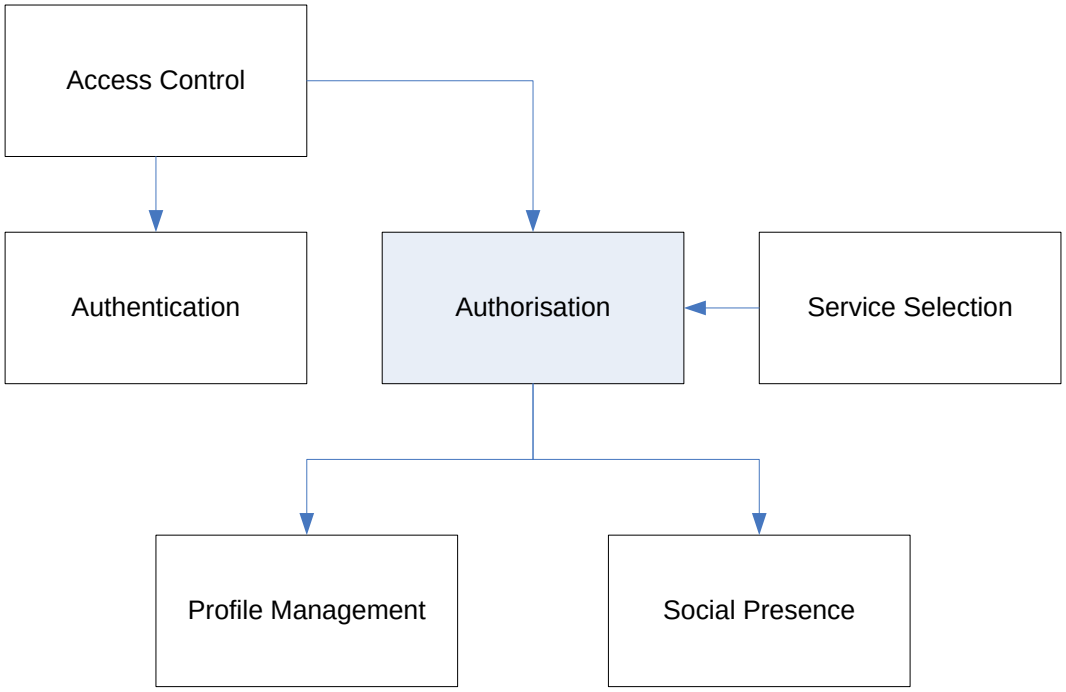


Figure 70 Authorisation

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

E.9 Date/Time Stamper

T_2

PICOS Principle (PP): 12, 23

PICOS Feature (PF): 1, 2, 10, 15

E.9.1 Purpose

The *Date/Time Stamper* provides an accurate and reliable date/time reference.

E.9.2 Description

Text, audio, picture and video in the online world are in digital form and easily modifiable. This gives rise to questions of how best to check when a document was created or last modified. Cryptographic processes, e.g. hash, MAC and digital signature functions allow changes to be detected, but they do not reveal the time of modification. For example, with intellectual property matters it is sometimes crucial to verify the date that the inventor first recorded the patentable idea, in order to establish its precedence over competing claims. PICOS can digitally time-stamp any documents so that it is infeasible for a date to be backdated or forward-dated.

Date and Time stamping must satisfy two fundamental requirements:

- It must be infeasible to timestamp a document with a date and time different from the present one
- It must be infeasible to change even a single bit of a time-stamped document without the change being apparent.

Many other components might find the Date/Time Stamper component useful, e.g. Feedback component, Event Logging component, Content Sharing (Importer/Exporter) component.

The Date/Time Stamper component adds a time-stamp to a document. It requires access to a stable date/time reference.

Example: RFC 3161: Time Stamping Protocol defines the entities involved (Requestor / Client and Time Stamp Authority (TSA) / Server), the message format and the transport protocol which permits communication between the entities. The following figures show the ‘time-stamp request’ and the ‘time-stamp verify’ phases.

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

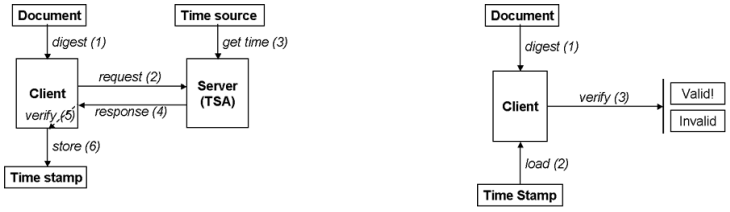


Figure 71 Example Time/Stamp protocol

E.9.3 Dependencies

Components that this component calls	Purpose
None defined at present	

Components that call this component	Purpose
Content Sharing	To record when content is imported and shared.
Event Logging	To record when events are written to the event log.
Feedback	To record when feedback was provided.

E.9.4 Drawing

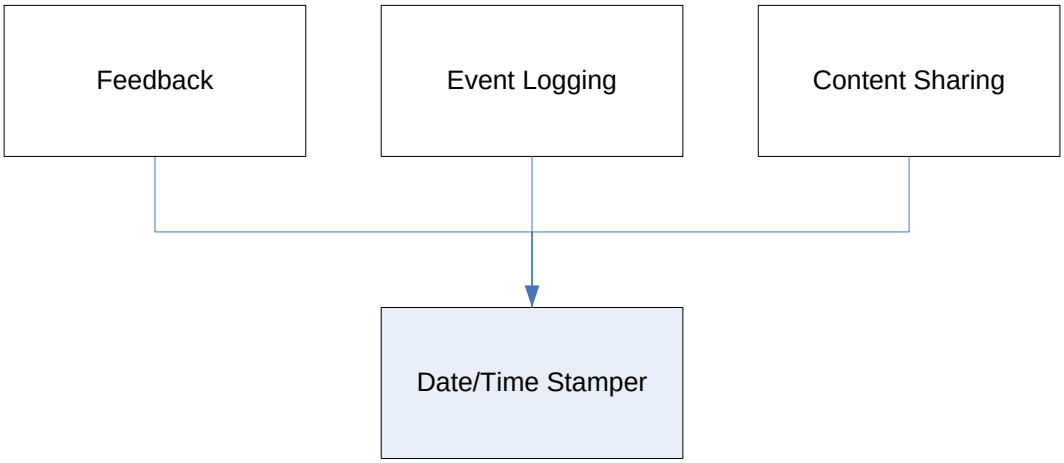


Figure 72 Date/Time Stamper

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

E.10 External Recommendation

T_2 PICOS$_{distinguishing}$ PICOS$_{research}$

PICOS Principle (PP): 6, 16, 22, 23

PICOS Feature (PF): 1

E.10.1 Purpose

The *External Recommendation* component acts as a gateway for recommendations that come from other communities or from external / non-trusted sources.

E.10.2 Description

The *External Recommendation* component establishes a common language or common ranking system that allows external recommendations to be interpreted in a common way. It would most probably be called by the *External Service Delivery* component. It allows internal and external recommendations (probably just reputation to begin with) to be compared on the same scale.

In the case of external reputation, this is managed in the same way as for a member by the *Reputation Management* component. It will be anonymised and recorded against the partial identity of the external entity using the *Profile Management* component.

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

E.10.3 Dependencies

Components that this component calls	Purpose
Profile Management	To record the reputation of the external entity.
Reputation Management	For reputation management service as used with members.

Components that call this component	Purpose
External Service Delivery	To check recommendations on external services.

E.10.4 Drawing

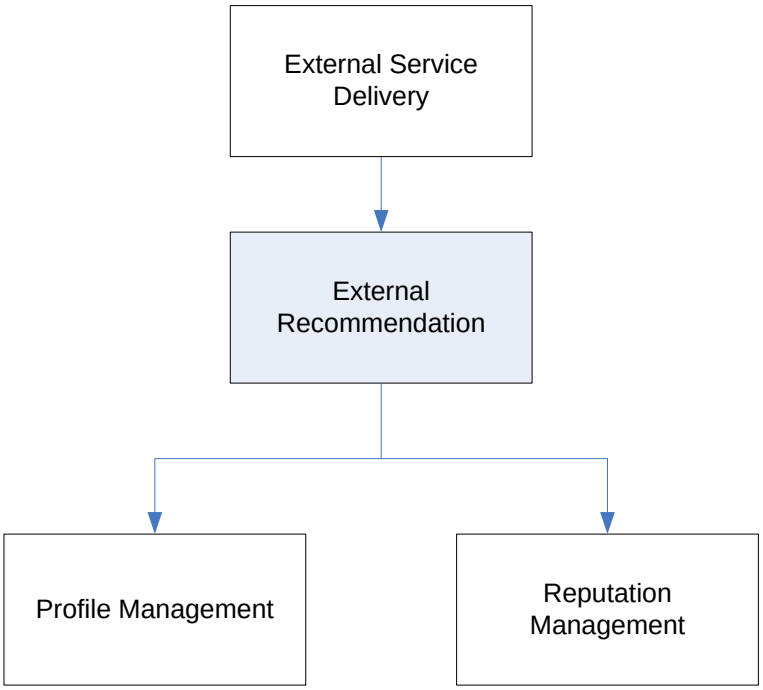


Figure 73 External Recommendation

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

E.11 External Service Delivery

T2 PICOSenhancing

PICOS Principle (PP): 6, 13, 17, 22

PICOS Feature (PF): 10

E.11.1 Purpose

The *External Service Delivery* component is responsible for ensuring that external service is delivered according to the level and quality of service previously defined and agreed with community operator/members. This component can also aggregate service to provide richer services to members.

E.11.2 Description

The *External Service Delivery* manages the interaction with external service providers. It controls how members access external services and limits the amount of member personal information using the *Data Minimisation* component. It also controls the delivery of content and notifications from the service provider to community members using the *Content Sharing* component.

Service aggregation can cover both the aggregation of the content the aggregation of services. At the content level, aggregation allows members to merge documents and live feeds to provide a common source of information. At the service level, aggregation takes internal and external service, ranging from full-scale applications to simple functions (code fragments), that can be combined into larger services. Web-based aggregation is also a possibility, e.g. Google Reader.

To enhance privacy, external service can be accessed anonymously using a partial identity specifically created by the *Partial Identity Manager* component.

A useful description of how external service delivery is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 6: External services

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

E.11.3 Dependencies

Components that this component calls	Purpose
Content Sharing	To allow content received from any external service provider to be shared with other members.
Data Minimisation	To reduce the information that a member shares with an external service provider.
Partial Identity Management	To anonymise the identity of the member accessing the external service.

Components that call this component	Purpose
Service Selector	By members requesting access to an external service.

E.11.4 Drawing

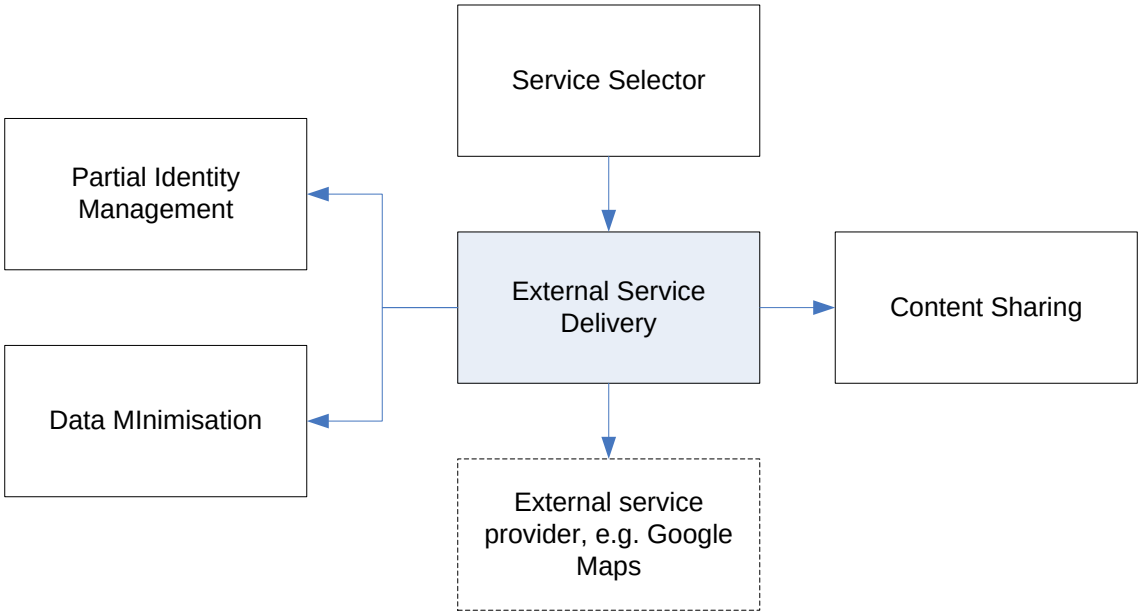


Figure 74 External Service Delivery

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

E.12 Feedback Management

T2 PICOSdistinguishing

PICOS Principle (PP): 5, 16, 23

PICOS Feature (PF): 1

E.12.1 Purpose

The *Feedback Management* component provides a route for members to supply feedback to the community.

E.12.2 Description

Feedback from members is vital in online communities, whether the community is provided for professional or leisure-time activities. Creative contribution from the membership is vital to the growth and success of any community, large or small. The more members are engaged (i.e. providing feedback) with the community, the stronger the community becomes. Members are also a valuable source for ideas. Capturing member feedback can lead to new, innovative community services.

The *Feedback Management* component is a service that:

- Collects feedback from contributors
- Creates and facilitates fellowship and one-to-one communication among community members
- Shares feedback and information provided by other members, and report on progress implementing new features which resulted from member user suggestions
- Allows customisation/innovations to meet the needs of community members
- Provides input into the reputation system, so that members who support the community through action or contribution can be rewarded with positive remarks

Feedback can take various forms, from simple 5-star ratings, karma rating through to personal recommendation. Feedback in this form is also referred to as reputation. Feedback is especially helpful in large communities where feedback can enhance trust in other members and the community as a whole. Reputation is automatically adjusted when feedback is received and can lead to increased privileges for the member concerned.

Privacy is always a concern, so the *Feedback Management* component restricts feedback to specified sub-communities or ensures that feedback is anonymous but accountable (subject to control to filter inappropriate feedback). Feedback is tagged to indicate the partial identity of member who provided the feedback.

The feedback process should ideally be self-managing, or managed by a 'leader' elected by the community (and the election could be based on feedback or reputation). Centralised monitoring of

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

content, the censorship of entries and control over the focus and activities of sub-communities should be avoided.

E.12.3 Dependencies

Components that this component calls	Purpose
Reputation Management	To record reputation information.

Components that call this component	Purpose
Service Selection	To allow members to provide feedback.

E.12.4 Drawing

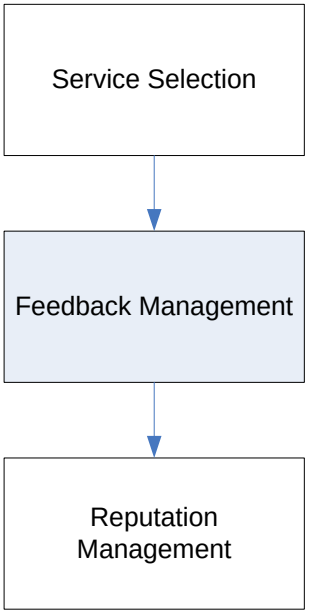


Figure 75 Feedback Management

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

E.13 Identity Translator

T2 PICOSdistinguishing

PICOS Principle (PP): 6, 13, 18

PICOS Feature (PF): 9, 13

E.13.1 Purpose

The *Identity Translator* component is an extension to the Identity Management component which deals with special situation concerning external identities.

E.13.2 Description

The *Identity Translator* component is an extension, i.e. a separate service, to the *Identity Management* component. Its purpose is to 'reconfigure' an identity to take account of a special situation surrounding the access to a service or external community, using the *External Service Delivery* component. For example, a member may have a preference set that states that their identity must be anonymised or reduced in 'richness' (i.e. some personal information removed) when they interact with any part of the community outside of their designated sub-community. The reason for this is that they do not want to excessively expose personal information in an environment which they do not consider trustworthy.

The *Identity Translator* component would most likely call on the Anonymisation component or the *Partial Identity Management* component to perform this request. Exactly what action the *Identity Translator* takes will depend on the policy set by the member and the community, the context of the situation and possibly other factors like member and community(ies) reputation.

Another reason for invoking the *Identity Translator* component is because part of the community cannot support the format of the identity used elsewhere. This may be true with a legacy system or possible a mobile client which has limited functionality. It may also be required during ad hoc interaction with other communities (possibly as a guest member).

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

E.13.3 Dependencies

Components that this component calls	Purpose
Data Minimisation	To reduce the 'richness' on personal data sent to the service provider.
Partial Identity Management	To create pseudonyms as alternative to personal identifiers, which should be less revealing of personal information. Note: the *Partial Identity Management* component may utilise the *Anonymisation* component.

Components that call this component	Purpose
External Service Delivery	To access an external service.

E.13.4 Drawing

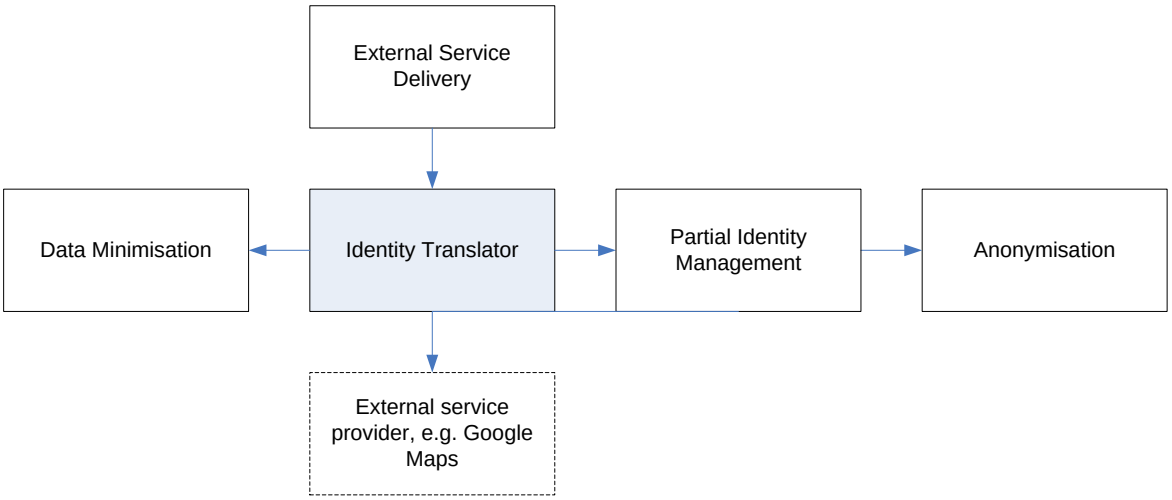


Figure 76 Identity Translator

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

E.14 Importer/Exporter

T1 PICOSenhancing

PICOS Principle (PP): 2, 3, 4

PICOS Feature (PF): 2, 5, 6, 10, 12

E.14.1 Purpose

The *Importer/Exporter* component is responsible for (mainly) allowing members to upload/download content.

E.14.2 Description

The *Importer/Exporter* component represents the interface for data exchange between the community and member. It provides for the synchronisation and backup of personal data, and the up-/downloading of content. By uploading contact data from an address book, e.g. Microsoft Outlook, it is possible to expand the PICOS address book or PICOS buddy list to include members from the mobile community. Additionally, an interface is available which allows the exchange of data with other communities, e.g. GoogleMail, Facebook, etc.

This *Importer/Exporter* component also supports the import/export of media (e.g. picture, video and sound files) and document (e.g. Microsoft Word documents, pdf files, etc.), so that content can be shared between members. Furthermore, the *Importer/Exporter* component supports the import/export of personal data from a mobile client, including address data and security settings. The component supports backup and migration of client devices.

Imported data may be manually or automatically 'tagged' with meta-data, and transferred to a predefined location for sharing with other members of the community, subject to access restriction being satisfied.

The *Importer/Exporter* makes extensive use of the *Content Sharing* component.

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

E.14.3 Dependencies

Components that this component calls	Purpose
Content Sharing	To 'tag' content, make content available to (share with) other members and to apply restriction on access to the content.

Components that call this component	Purpose
Service Selection	In response to a member request to import/export content.

E.14.4 Drawing

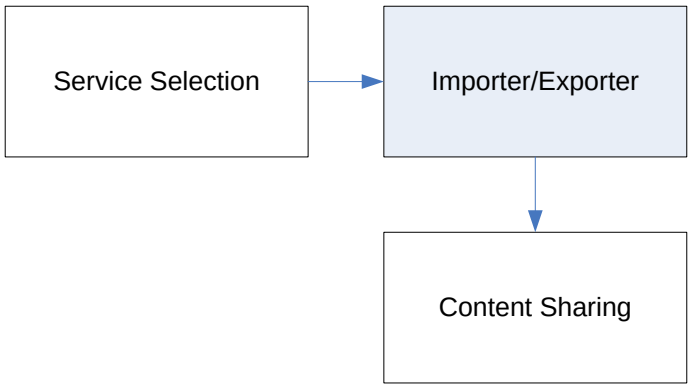


Figure 77 Importer/Exporter

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

E.15 Location Sensor

T2 PICOSenhancing

PICOS Principle (PP): 10

PICOS Feature (PF): 4, 8

E.15.1 Purpose

The *Location Sensor* reports the current location of the member.

E.15.2 Description

The *Location Sensor* component provides an interface to retrieve the current location of a member. The location can either be determined by the member (client) device, e.g. using a GPS receiver, or by the network, e.g. cell-based location.

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

E.15.3 Dependencies

Components that this component calls	Purpose
None defined at present	

Components that call this component	Purpose
Access Control	As part of authorisation during access control.
Authorisation	As part of authorisation during service selection.

E.15.4 Drawing

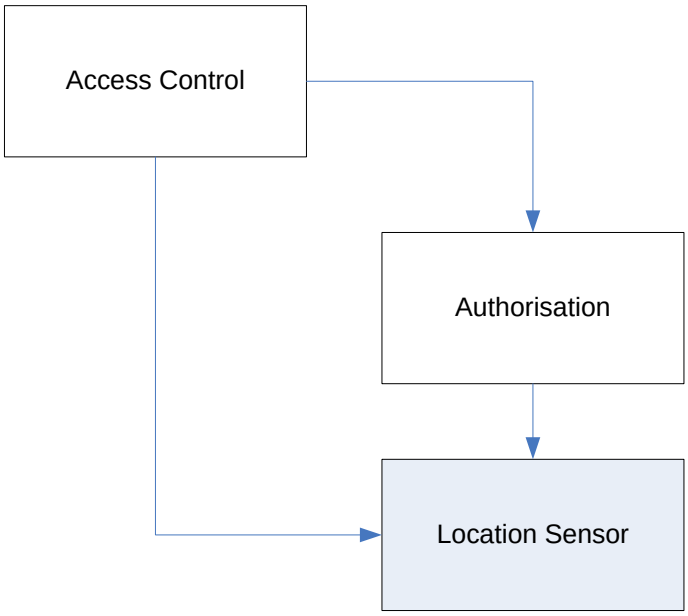


Figure 78 Location Sensor

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

E.16 Notification

T2 PICOSenhancing

PICOS Principle (PP): 10, 13

PICOS Feature (PF): 5, 11, 12

E.16.1 Purpose

The *Notification* component communicates with members in response to a member or community initiated event.

E.16.2 Description

For a variety of reasons, members or the community operator need to notify other members that something within the community has changed, or that an action must be taken. For example, when a member contributes content to the community they will want to notify all members who are permitted to see the content that the content is available. The *Social Presence* component may also need to call the *Notification* component to alert selected members to a change in status of another member.

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

E.16.3 Dependencies

Components that this component calls	Purpose
None defined at present	Notification is currently considered to be an internal function of the community messaging system.

Components that call this component	Purpose
Social Presence	To alert a change in social presence, e.g. location.
Content Sharing	To alert members of an import of content that they are entitled to access.

E.16.4 Drawing

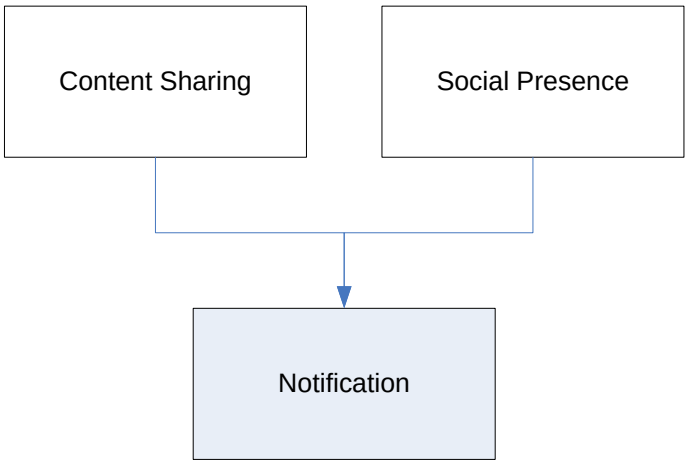


Figure 79 Notification

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

E.17 Partial Identity Management

T_2 | $PICOS_{distinguishing}$ | $PICOS_{research}$

PICOS Principle (PP): 11, 18

PICOS Feature (PF): 1, 3

E.17.1 Purpose

The *Partial Identity Management* component creates partial identities that enable members to interact with the community.

E.17.2 Description

The role of the *Partial Identity Management* component is to enable members to utilise one or more partial identities as they interact with other community members. A partial identity is an identity that includes some but not all personal attributes. For example, a partial identity may consist of a name and telephone number, or more likely will be a pseudonym. The latter has the advantage of affording greater privacy.

For reasons of accountability and community management, it may be necessary to link all partial identities that relate to a single individual under a common identity, in PICOS called the root identity. The ability to link partial identities for an individual would be restricted, either to the community operator or an external trusted intermediary (or a law enforcement authority).

Every member has at least one partial identity, which is created when they register with the community and subsequently when they request for additional partial identities. The reason for requesting additional partial identities is so that members can interact with the community in multiple ways.

Every partial identity has a profile, preferences and a reputation, and to other members appears like a unique member.

Partial identities provide members with access to the community and community services.

A useful description of how partial identifiers are employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 1: Registration
- PICOS Use Case 2: Accessing the community
- PICOS Use Case 4: Multiple Partial Identities
- PICOS Use Case 5: Reputation

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

E.17.3 Dependencies

Components that this component calls	Purpose
Anonymisation	To create the partial identity (a pseudonym) endorsed by the community.
Profile Management	To assign the partial identity a profile.

Components that call this component	Purpose
Registration	When registering as a member of a community, an initial partial identity is automatically created.
Service Selection	When a member wants to create an additional partial identity.

E.17.4 Drawing

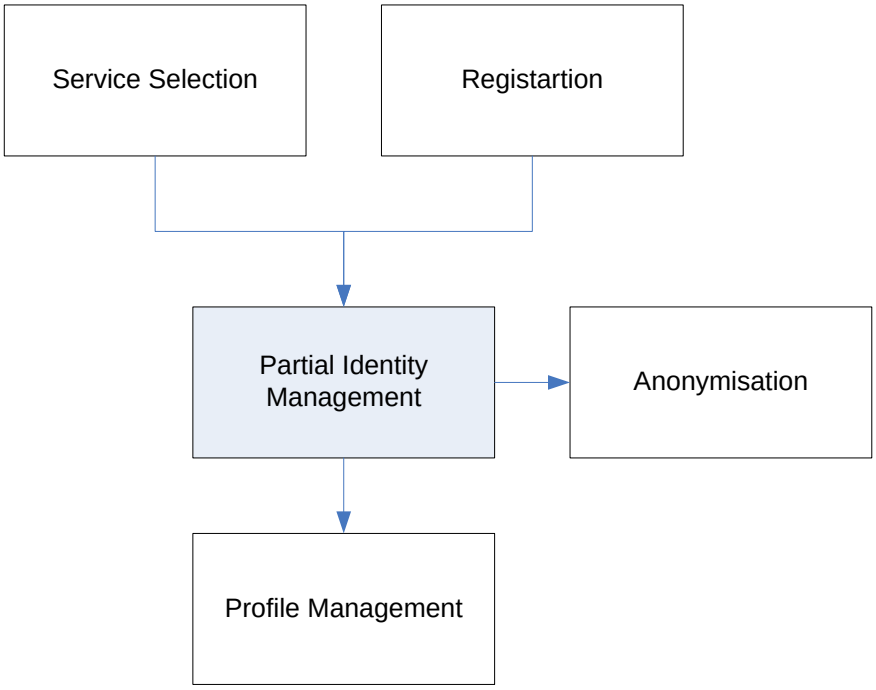


Figure 80 Partial Identity Management

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

E.18 Payment Services

T_2 PICOS$_{enhancing}$

PICOS Principle (PP): 3, 4, 9, 13

PICOS Feature (PF): 9

E.18.1 Purpose

The *Payment Services* component provides access to external payment service, e.g. Visa, MasterCard, PayPal. It is specifically included in the PICOS architecture because PICOS addresses privacy issues that arise through advertising. In all other respects, the *Payment Services* component is similar to other externally provided services.

E.18.2 Description

The *Payment Services* component enables members to purchase services offered by the community operator, or offered by an external service provider that has advertised services to the community. Such a service is accessible the *External Service Delivery* component.

Several payment methods should be catered for, e.g. Visa, MasterCard, PayPal, thus the payment service is essentially outsourced. The community operator ensures a common user experience and integration between the community and the supplier of the service being purchased.

Payment problems are resolved between the member(s) concerned and the external payment service provider.

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

E.18.3 Dependencies

Components that this component calls	Purpose
External Payment Delivery	To gain access to the payment service provider's system.

Components that call this component	Purpose
Service Selection	When a member wants to make a payment for a service (possibly including and external service).

E.18.4 Drawing

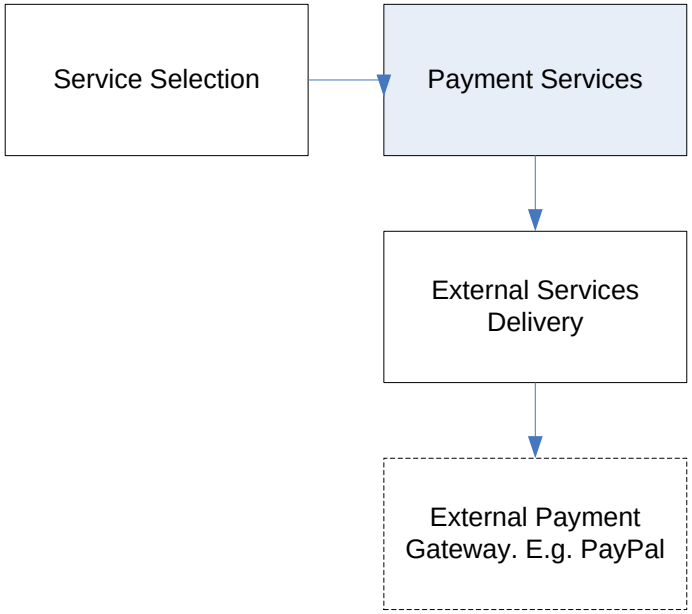


Figure 81 Payment Services

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

E.19 Preparation Area

T1 PICOSdistinguishing

PICOS Principle (PP): 5, 10

PICOS Feature (PF): 14

E.19.1 Purpose

The *Preparation Area* component provides a secure area for members to create and manage content before sharing with the community.

E.19.2 Description

The *Preparation Area* component, also referred to as personal space, provides an area where members can experiment, get used to the community and experience what the community has to offer without any personal risk. It enables members to build trust in the community and its services.

The preparation area is presented as a service, and may be available to Guest members if the community policy permits.

A parallel can be drawn with Web 2.0. Web 2.0 is designed to allow members to easily establish personal workspaces on the Internet. The same principle applies to a PICOS community. In Web 2.0, aspects of personal and public spaces are closely intertwined. Members are able to choose for themselves, and effectively trade privacy for greater social interaction.

Only the owner of the personal space has access; it is not visible to any other community member or operator. It is not audited and no history is maintained. However, it is possible for members to transfer personal information from the preparation area into the main body of the PICOS community, at which point the information is managed using the controls that PICOS provides for the community.

The functionality that supports the preparation area can be provided locally, on the client platform, or centrally by the community. The latter is potentially less secure but more convenient for client platforms with limited capabilities.

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

E.19.3 Dependencies

Components that this component calls	Purpose
None defined at present	The preparation area can be considered as a duplicate PICOS community, possibly provided in a trusted location or by a Trusted Third Party (TTP).

Components that call this component	Purpose
Service Selection	To allow a member to experiment with PICOS functionality is a safe situation.

E.19.4 Drawing

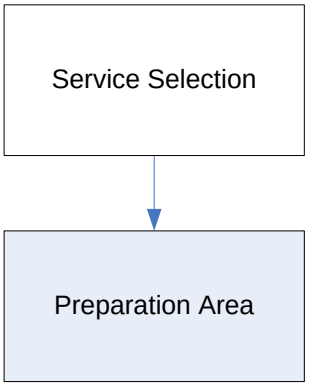


Figure 82 Preparation Area

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

E.20 Privacy Advisor

PICOS D4.2 new/updated component

T2 PICOS distinguishing PICOS research

PICOS Principle (PP): 3, 4, 8

PICOS Feature (PF): 2, 10

E.20.1 Purpose

The *Privacy Advisor* informs members if the action they are about to perform will place their privacy at risk.

E.20.2 Description

The *Privacy Advisor* is perhaps best thought of as a member's best buddy. It is designed to provide guidance of privacy related matters that may affect a member as they interact with the community. Privacy (and trust) is subjective, and it is often difficult to find a single 'right answer' to questions and concerns about privacy. One of the challenge is one of understanding what information a member values most. The role of the *Privacy Advisor* component is to present facts about the community that have a bearing on privacy. Along with the member's privacy preferences and profile, it should be possible to offer advice to the member. Therefore, *Profile Management* and *Reputation Management* components are likely to be involved.

This is probably best described as an 'advanced component', where further research is necessary. For this first version of the architecture, it is important to create a 'place holder' for this type of functionality, and to offer a simplified service consisting of perhaps general community information (number of member, recent activity) and events that relate directly to information that a member has contributed to the community for the benefit of others.

The *Privacy Advisor* component may be activated for a variety of reasons, e.g. by the *Service Selection* component, *External Service Delivery* component and *Scenario Management* component. It may also play an important role in negotiating trust, i.e. the *Trust Negotiation* component.

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

E.20.3 Dependencies

Components that this component calls	Purpose
Profile Management	To obtain information about the entity involved.
Reputation Management	To obtain information about the entity involved.

Components that call this component	Purpose
External Service Delivery	To advise the member on the action that they are about to perform.
Scenario Management	To provide context information to help members make decisions about the exposure of an identity (or partial identity), the sharing of information and the use of community services.
Service Selection	To advise the member on the action that they are about to perform.
Trust Negotiation	To advise the member on the action that they are about to perform.

E.20.4 Drawing

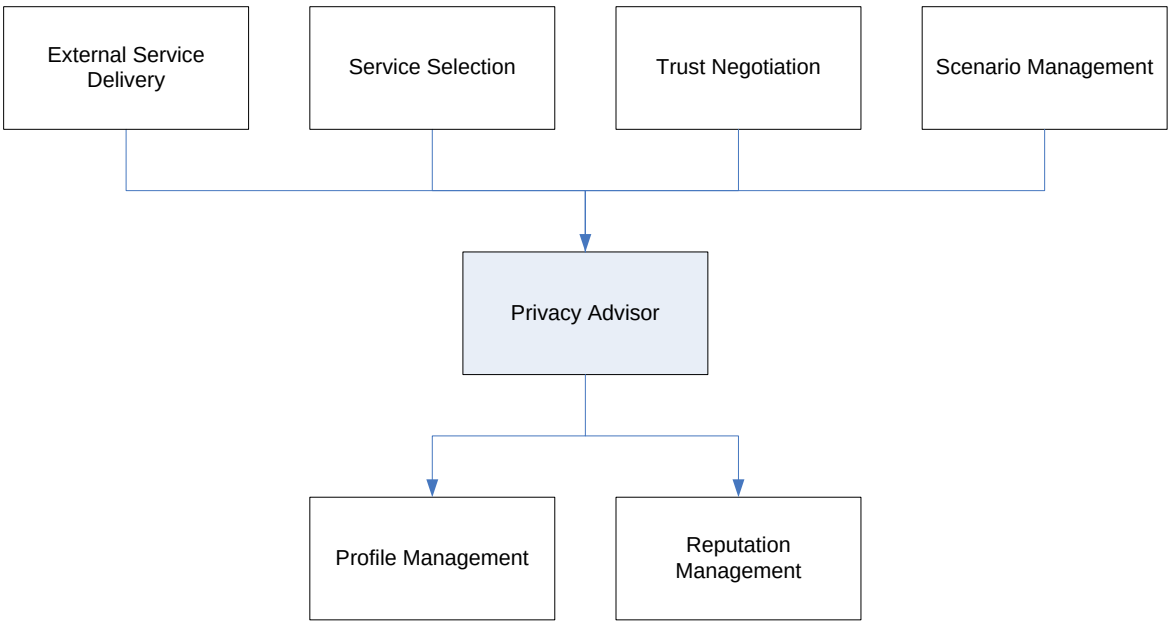


Figure 83 Privacy Advisor

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

The improvement or new functionality added in Gamers Community, with regard the first prototype, is to scan the asynchronous messages content besides scanning the profile attributes.

This means that the Privacy Advisor will check/scan as the Threads Post content as asynchronous message content and in case end-user is sending sensitive information which is included into the User's Profile, then it will send a notification to the user, warning him about the risks that it implies, and he will can react and decide whether he want to go ahead and send the information anyway, or cancel the sending.

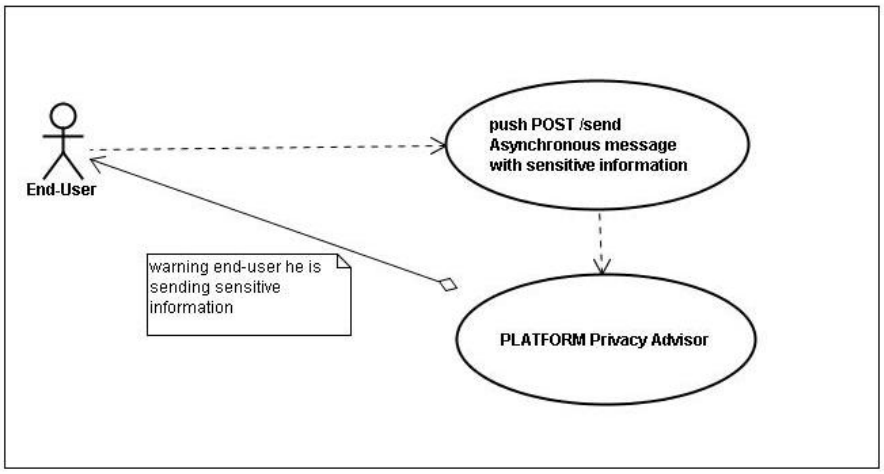


Figure 84 Privacy Advisor Use Case

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

E.21 Recruitment

T2 PICOSdistinguishing

PICOS Principle (PP): 21, 23

PICOS Feature (PF): 1

E.21.1 Purpose

The *Recruitment* component provides a way for existing members to recommend prospective members for membership of the community.

E.21.2 Description

The *Recruitment* component provides functions to enlist new members, based on recommendations from existing members and reputation. Another source of recommendation is a Trusted Third Party (TTP) or intermediary, via the *TTP Management* component, which would vouch for the prospective member. Thirdly, the recommendation may come from another community, perhaps via the *External Recommendation* component.

One of the criterion that the Authentication component accepts as evidence is a completed application form. An option is for this form to be endorsed (similar to a sponsor) by and existing member. The *Recruitment* component could support this process.

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

E.21.3 Dependencies

Components that this component calls	Purpose
Authentication	To support a prospective member's application form.

Components that call this component	Purpose
External Recommendation	To recommend a prospective member for membership.
TTP Management	To recommend a prospective member for membership.

E.21.4 Drawing

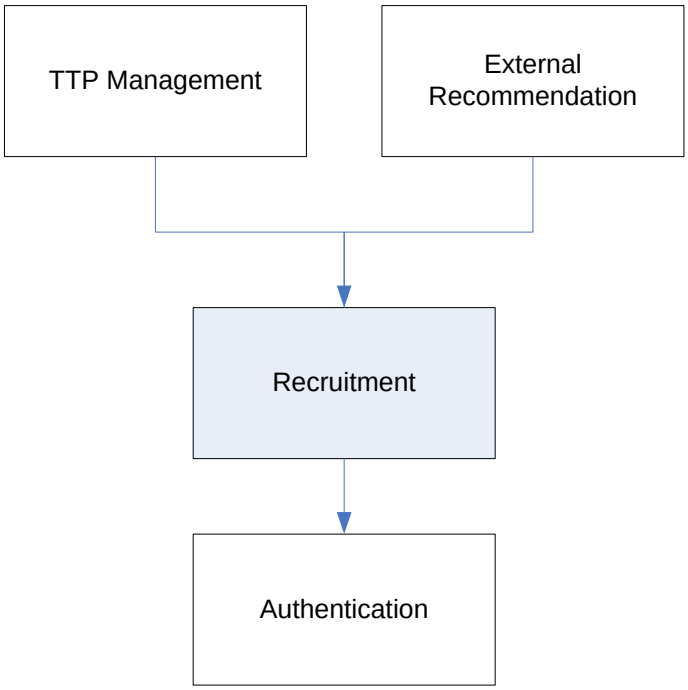


Figure 85 Recruitment

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

E.22 Reputation Management

T_2 | $PICOS_{enhancing}$ | $PICOS_{research}$

PICOS Principle (PP): 6, 22, 23

PICOS Feature (PF): 1

E.22.1 Purpose

The *Reputation Management* component is used to provide an indication of the trustworthiness of an entity (typically a member).

E.22.2 Description

Reputation is an important mechanism for building trust between community members, and forms the basis for making recommendations. Reputation is based on member performance and typically derived from feedback and recommendation from other members. Recommendations are transitive, in that member A recommends member B to member C, but member C has no firsthand experience of member A. (Trust is often said to be transitive too, i.e. A trusts B, and B trusts C, therefore A trusts C). From this principle, a hierarchy of member recommendations can be created and maintained as a basis for trust between the members.

The *Reputation Management* component is responsible for handling reputation received from members. The exact process requires further research, but one possibility is for the *Reputation Management* component to maintain a recommendation graph, which represents links between members. Reputations can be added/removed from the graph. In order to build trust it may be necessary to maintain a history showing the 'lifetime of a reputation', so that members can observe how it has evolved.

Reputation is not only concerned with the reputation of other members. It is equally concerned with reputation of subjects/topics/items/activities, in fact anything relevant to the community. For example, in the angling community reputation might include fishing location, tackle, bait, conditions and external angling services.

Reputation information is stored in the profile of the entity (member) to which it relates, using the *Profile Management* component. It may be requested by various components, but in particular the *External Recommendation*, *Privacy Advisor* and *Trust Negotiation* components.

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

E.22.3 Dependencies

Components that this component calls	Purpose
Profile Management	To record reputation information on the entity concerned.

Components that call this component	Purpose
External Recommendation	To obtain reputation information on the entity concerned.
Privacy Advisor	To obtain reputation information on the entity concerned.
Trust Negotiation	To obtain reputation information on the entity concerned.

E.22.4 Drawing

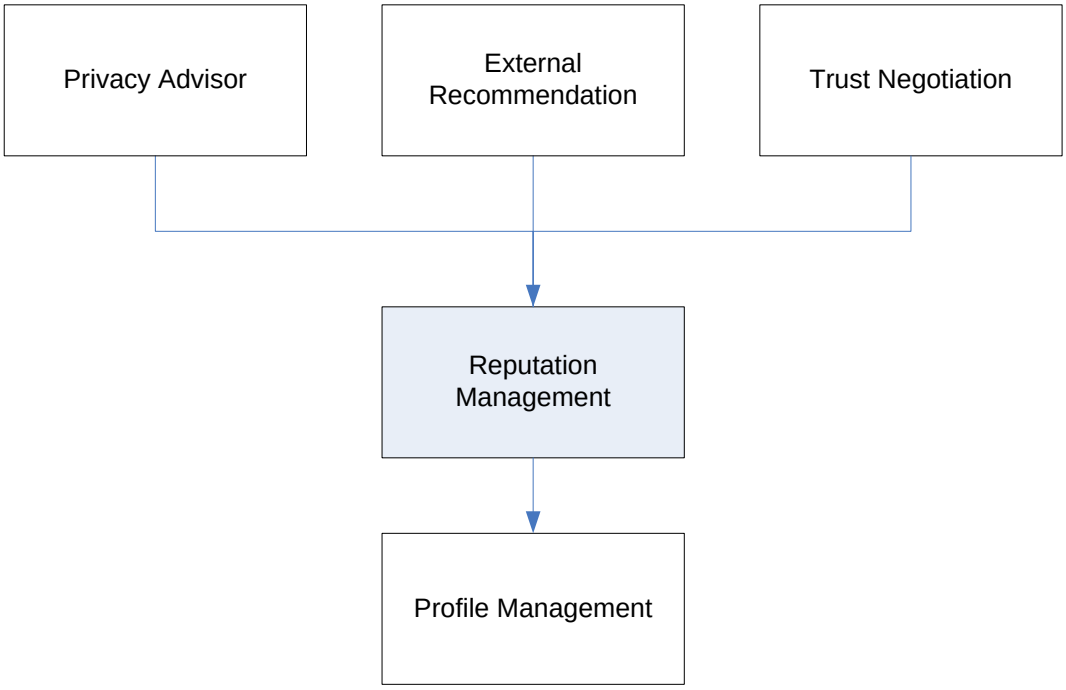


Figure 86 Reputation Management

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

E.23 Scenario Management

T2 PICOSdistinguishing

PICOS Principle (PP): 8, 11, 23

PICOS Feature (PF): 2

E.23.1 Purpose

The *Scenario Management* component provides context information to members, sufficient to help them make decisions about the exposure of an identity (or partial identity), the sharing of information and the use of community services.

E.23.2 Description

The *Scenario Management* component determines the current context and assesses its relevance to maintaining privacy. It also assesses the impact of a changing context and the implication of trust policies intended to protect sensitive information.

In an online community it is often difficult to determine context (i.e. determine or understand a scenario), since members are not aware of other members, services or third parties who might be observing or collecting data, e.g. to analyse virtual behaviour. Therefore, mechanisms are required that detect and communicate something about the environment in which members operate.

There are (at least) four metrics that can be observed in a typical scenario, and which could be used to indicate risk (and therefore impact on trust and privacy):

- The complexity of the relationship between members (including members of other communities), and the use of services (especially third party provided services) can suggest the level of control, or the ability to enforce personal privacy policies
- The sensitivity of the data being shared or processed is another indicator. The more sensitive and extensive the data, the greater the impact of exposure and the need for tighter control.
- A third metric is the reputation of other members involved in the scenario. The strength of authentication may also have a bearing on the trustworthiness on those involved in the scenario. This can be extended to the reputation of services that support data processing and sharing.
- A fourth metric is the communication medium over which information is shared.

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

E.23.3 Dependencies

Components that this component calls	Purpose
Privacy Advisor	To provide input to the privacy advice process.

Components that call this component	Purpose
External Service Delivery	To advise the member on the action that they are about to perform.
Service Selection	To advise the member on the action that they are about to perform.
Trust Negotiation	To advise the member on the action that they are about to perform.

E.23.4 Drawing

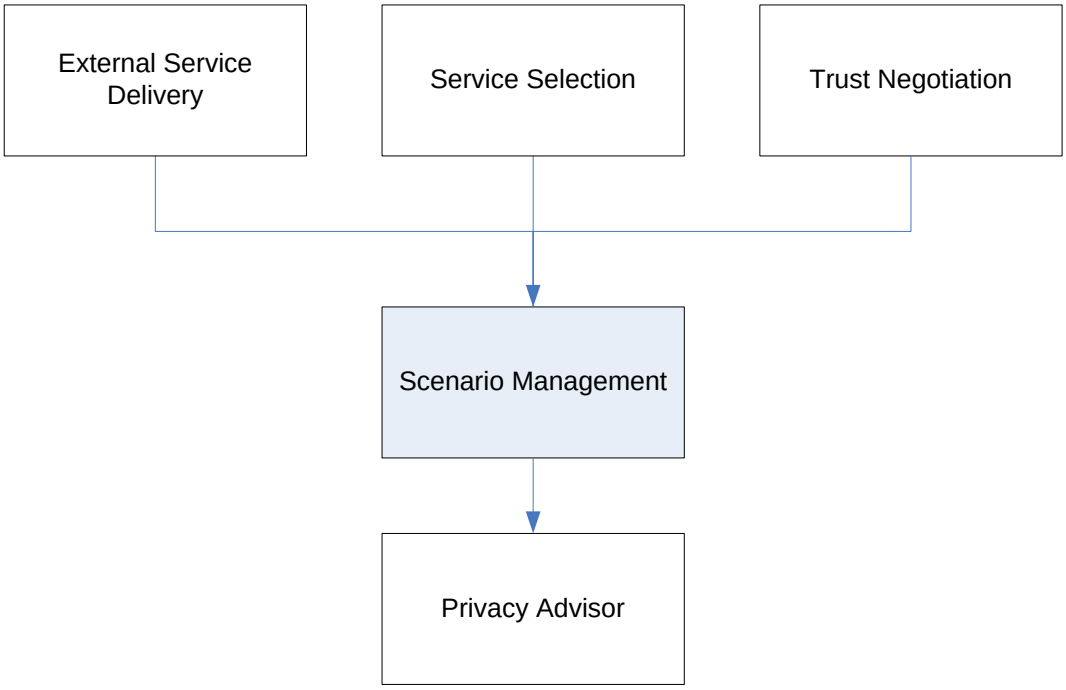


Figure 87 Scenario Management

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

E.24 Service Selection

T1 PICOSenhancing

PICOS Principle (PP): 11, 13, 17

PICOS Feature (PF): 9, 13

E.24.1 Purpose

The *Service Selection* component presents the available service to the member.

E.24.2 Description

Once a member has gained access to the community via the *Access Control* component, they are presented with the set of service that they can access according to their privileges. Privileges are set in their profile by the *Profile Management* component.

In addition, restrictions on the service available to the member may be imposed by the *Social Presence* component, and by the community policy as defined by the *Policy Management* component.

E.24.3 Dependencies

Components that this component calls	Purpose
Policy Management	To determine the services that the member can access
Profile Management	To determine the services that the member can access.
Social Presence	To determine the services that the member can access.

Components that call this component	Purpose
Access Control	To access a service.

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

E.24.4 Drawing

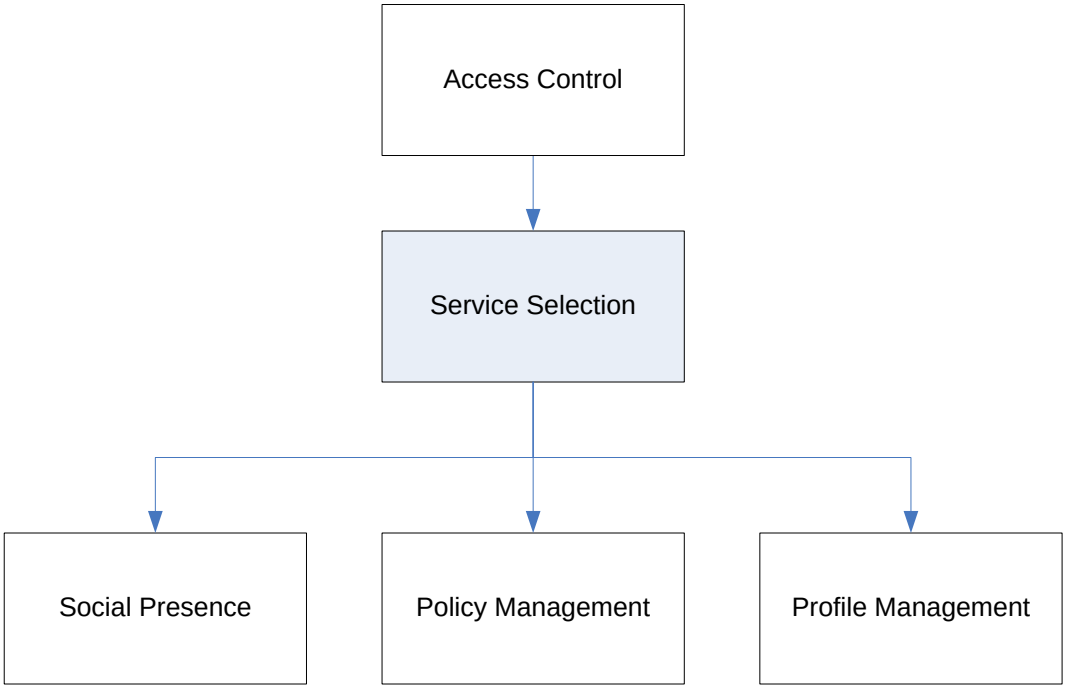


Figure 88 Service Selection

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

E.25 Social Presence

T2 PICOSdistinguishing

PICOS Principle (PP): 10

PICOS Feature (PF): 8

E.25.1 Purpose

The *Social Presence* component controls the visibility of a member to other members in the community.

E.25.2 Description

Social presence is defined as the willingness and ability of a member to communicate with other members in the community. Social presence also expresses a member's reachability and willingness to share current status information.

The *Social Presence* component accepts, stores, and distributes social presence information to other members who are interested.

Example: A presence service can be built using several protocols (models), e.g. SIP, RPC, RMI. Taking SIP as an example, and noting that in SIP members are referred to as 'watchers', then the main entities involved in a social presence service would be:

- Watcher: A member (Client_A) that wants to know the presence of another member. In order to obtain this information, the watcher creates a SUBSCRIBE request, and as long as the watcher subscription state is active, a NOTIFY message will be received any time there is a status change of the watched member (Client_B).
- Presence User Agent (PUA): A Presence User Agent manipulates presence information to extract a presence (for a member). This manipulation can be the side effect of another action (e.g. sending a SIP REGISTER request to add a new Contact) or can be done explicitly through the publication of presence documents.
- Presence Agent (PA): A Presence Agent is a SIP User Agent which is capable of receiving SUBSCRIBE requests, responding to them, and generating notifications of changes in presence state. A Presence Agent must have knowledge of the presence state of the member. This means that it must have access to presence data manipulated by PUAs for member. One way to do this is by co-locating the PA with the proxy, as shown below as P-CSCF).
- Presence Server: A presence server is a physical entity that can act as either a Presence Agent or as a Proxy Server, responding to SUBSCRIBE requests. When acting as a PA, it is aware of the presence information of the member. When acting as a Proxy Server, the SUBSCRIBE requests are 'proxied' to another entity which may act as a PA.

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

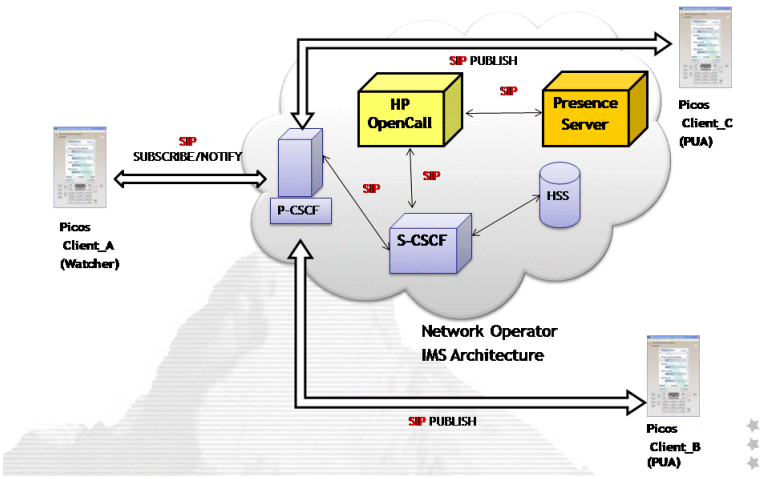


Figure 89 Example of Social Presence implementation using SIP

In the figure above, when an Client_A wishes to know the social presence of another member (e.g. Client_B), it sends a SIP SUBSCRIBE request . This request identifies the watched member in the Request-URI (Client_B URI). This request eventually arrives to the Presence Server, and is first authenticated and then authorised.

Once the Presence Server has authorized the subscription it sends an immediate NOTIFY message containing the state of the watched member (Client_B) and the subscription. The presence state may be bogus, in the case of a pending subscription (indicating offline). This is to protect the privacy of the watched member, who may not want to reveal that they have not provided authorisation to the watcher. As the state of the watched member changes, the Presence Server generates NOTIFY messages containing the new state, and notifies all subscribers (and authorised) watchers members subscriptions.

A useful description of how social presence is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 7: Presence

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

E.25.3 Dependencies

Components that this component calls	Purpose
Consent Management	To determine is the member wishes their social presence to be made available to other members, and if so then which members (or all).
Location Sensor	To obtain the current location of the member.
Profile Management	To obtain other social presence information about the member.

Components that call this component	Purpose
Service Selection	To obtain the social presence of a member.

E.25.4 Drawing

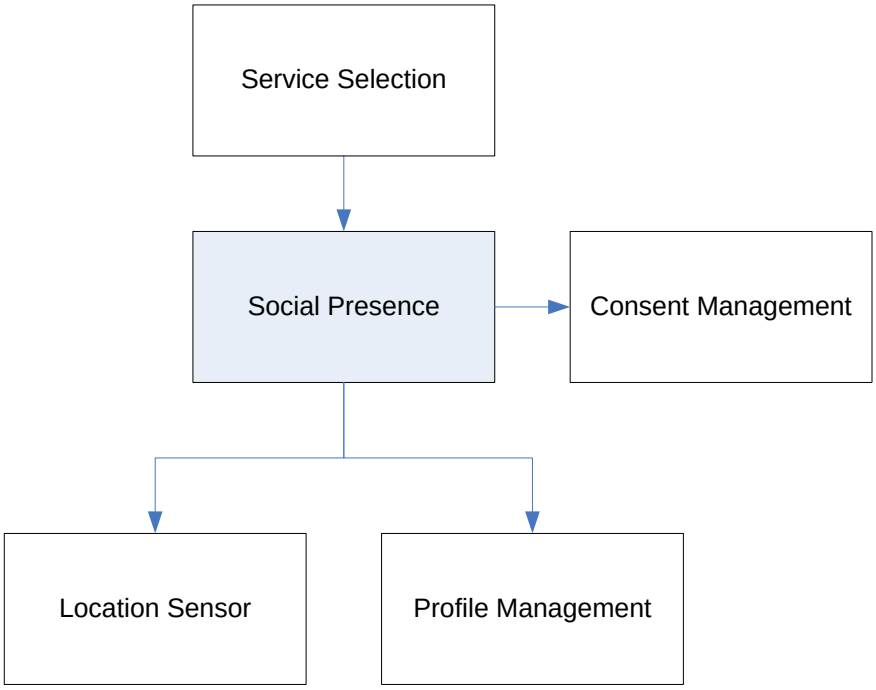


Figure 90 Social Presence

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

E.26 Trust Negotiation

T_2 PICOS$_{distinguishing}$ PICOS$_{research}$

PICOS Principle (PP): 6, 16, 22, 23

PICOS Feature (PF): 1, 15

E.26.1 Purpose

The *Trust Negotiation* component facilitates the establishment of a feeling of trust between two members.

E.26.2 Description

When members engage with others they do so as a conversation, where one gathers information about the character (desirable qualities) of the other. This forms the basis of trust. Initially trust is low, but is built up over time as more 'personal' information is exchanged. Whether it is correct to call this a negotiation is not clear, but clearly a protocol exists which governs the transfer (or not) of information.

The knowledge built-up about the other member consists in part of reputation, a matching of profile (a profile is intended to express personal attitude to privacy) and personal preferences. A goal might be for members to relax their preferences as they become more comfortable with those whom they interact. PICOS could encourage this to encourage broader interaction across the community.

The *Trust Negotiation* component establishes a shared level of trust between members. The *Trust Negotiation* component may be used when forming a new sub-community to establish membership, or to identify members with a similar trust profile who may be willing to interact with one another.

The component may be called as a member service via the Service Selector component, or by the *Privacy Advisor* component.

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

E.26.3 Dependencies

Components that this component calls	Purpose
Profile Management	To examine mutual trust.
Reputation Management	To use reputation as a basis for trust.
Sub-community Management	To create sub-community in which further trust can be established.

Components that call this component	Purpose
Privacy Advisor	To use the trust negotiation process to discover level of trust and then advice on privacy exposure.
Service Selection	When a member wishes to develop a trust with another member.

E.26.4 Drawing

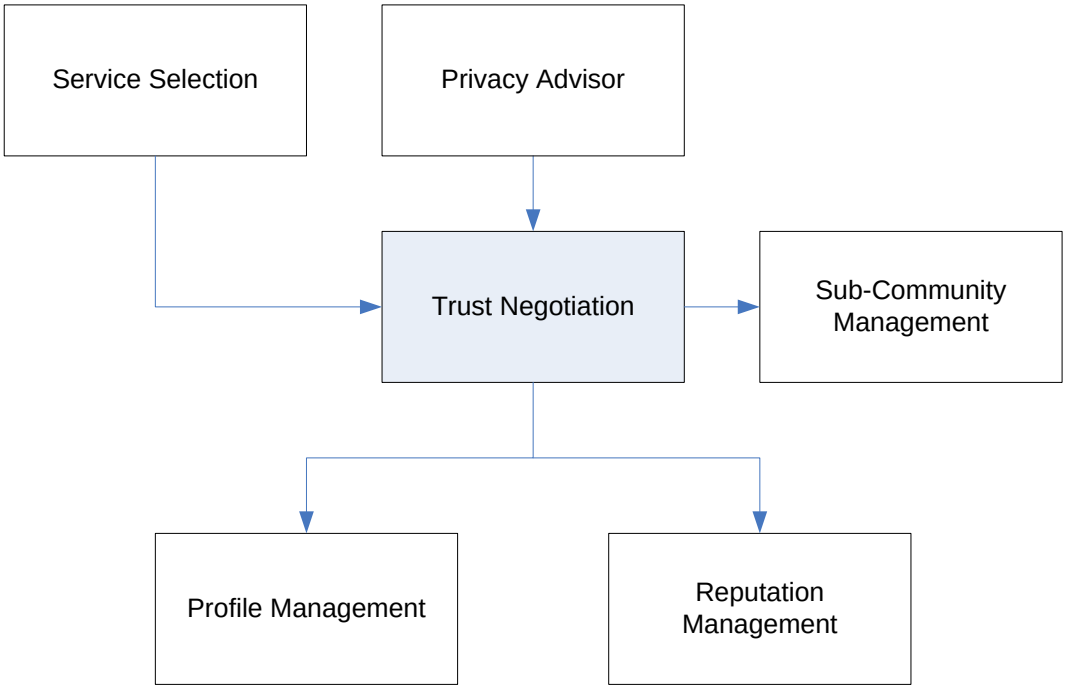


Figure 91 Trust Negotiation

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

E.27 TTP Management

T_2 PICOS$_{enhancing}$

PICOS Principle (PP): 1, 2, 6, 12, 22

PICOS Feature (PF): 1, 3, 9, 13, 15

E.27.1 Purpose

The *TTP Management* component provides the interface between the community and a trusted third party. It is most likely to be called as a result of a member selecting an external service, but may also be called for federated access or single sign-on by the *Access Control* component.

E.27.2 Description

A community may need the services of an external trust authority to endorse identities. For example, an external TTP (e.g. a Certification Authority (CA)) binds a real identity to a public key, having first proved that the member has proved 'ownership' of the corresponding private key. Other TTPs may provide law enforcement, non-repudiation or system checking services. Access to the *Cryptography / Key Management* component may be required.

Communities that offer non-repudiation with legal consequence must enlist the support of TTP that follows a standard of legal protocol for certificate issuance. They are likely to be regulated, and have the power (but not necessarily the authority) to 'break' that anonymity of community members. Normally, CAs honour the wishes of the member, but if the member is involved in an illegal activity or breaches community policy, the TTP may be required to reveal the member's real identity.

The TTP Management component therefore provides the connection to TTPs for operation (use by members) and administrative purposes (use to create and exchange endorsement information).

Since the TTP services the needs of the whole community it will operate according to policy set by the *Policy Management* component.

A TTP is a useful source of recommendation for recruiting new members, thus the *TTP Management* component provides a link to the *Recruitment* component.

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

E.27.3 Dependencies

Components that this component calls	Purpose
Cryptography / Key Management	To manage private or shared keys, and for key generation.
Policy Management	For community-wide operating practices relating to TTP.

Components that call this component	Purpose
Authentication	To validate federated identities.
External Service Delivery	Following a request to administer the TTP interface.
Recruitment	For external recommendation of new member for recruitment.

E.27.4 Drawing

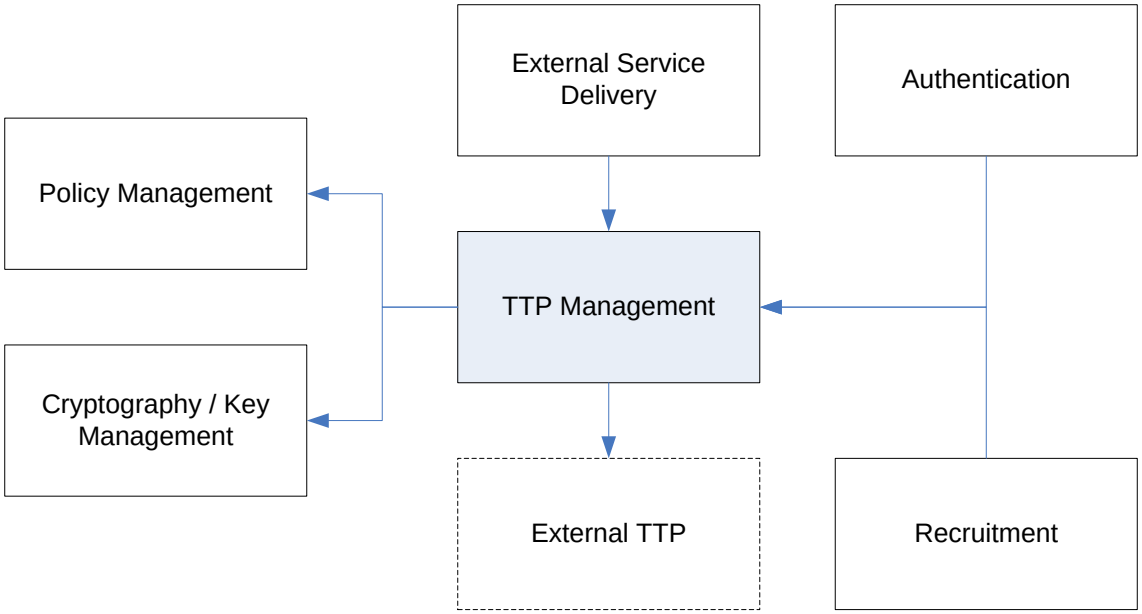


Figure 92 TTP Management

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

E.28 Accountability

T_2 $PICOS_{distinguishing}$ $PICOS_{research}$

PICOS Principle (PP): 1, 17

PICOS Feature (PF): 3, 15

E.28.1 Purpose

The *Accountability* component holds members accountable for their actions.

E.28.2 Description

The *Accountability* component monitors the behaviour of members to build trust confidence in the community, by attempting to detect dishonest activities. It can be thought of as the social conscience of the community. It is specifically engineered to detect activities that indicate fraudulent or inappropriate activity.

Information is collected from a variety of sources within the PICOS community. This information is analysed against predefined behaviour profiles. The results assist with community management and law enforcement, and feed into the reputation Management. On the basis of collected information (not defined yet) they are assessable.

The consequence of dishonest behaviour may be limited to the scope of the community, or may entail legal consequences. Identifying members in a community that aims to preserve privacy and protect identity has additional challenges. Where an action is performed under a pseudonym (or anonymously), the co-operation of an external Trusted Third Party (TTP) may be required in order to resolve the real identity behind the pseudonym. However, sometimes it is not necessary to discover the real identity of a pseudonymous/anonymous member in order to rectify an action or reprimand a member.

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

E.28.3 Dependencies

Components that this component calls	Purpose
Service Selection	For monitoring purposes.

Components that call this component	Purpose
Audit	To gather evidence.
Reputation Management	To gather evidence.
Event Logging	To gather evidence.

E.28.4 Drawing

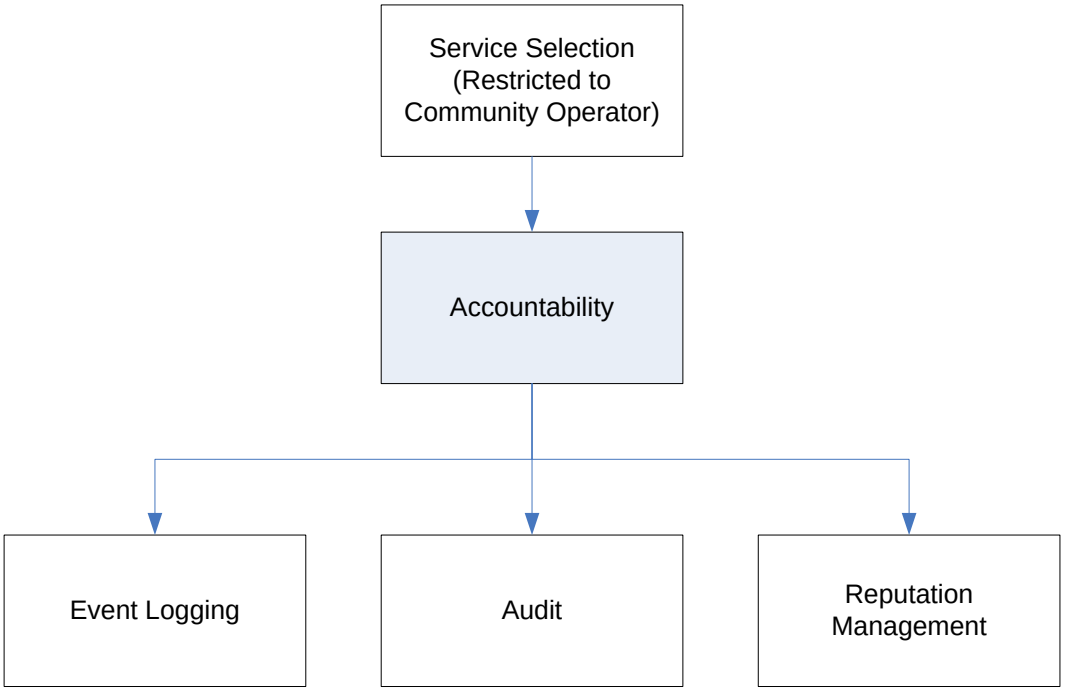


Figure 93 Accountability

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

E.29 Audit

T1 PICOSenhancing

PICOS Principle (PP): 1, 14

PICOS Feature (PF): 1, 15

E.29.1 Purpose

The *Audit* component provides easy access to information that may need to perform an internal or external audit of the community.

E.29.2 Description

The *Audit* component works alongside the Event Logging component, creating a record on community activities that are required for community monitoring activities.

For example, it may be necessary to examine member accounts to check on authentication mechanisms, roles and rights. It may also be necessary to examine system logs to check compliance with legal and regulatory requirements.

The data examined is collected from many sources, e.g. membership (lifecycle) management (including registration and access control), use of sensitive functions (e.g. tagging, payment services), and the general administration of the community (event logging).

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

E.29.3 Dependencies

Components that this component calls	Purpose
Event Logging	To gather data about the community.

Components that call this component	Purpose
Service Selection	To gain access to Audit tools.

E.29.4 Drawing

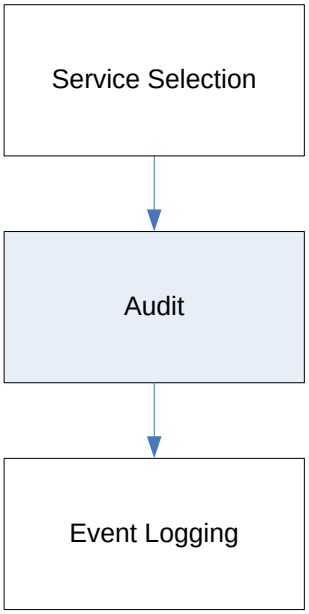


Figure 94 Audit

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

E.30 Event Logging

T2 PICOSenhancing

PICOS Principle (PP): 1, 5, 14, 20

PICOS Feature (PF): 1, 15

E.30.1 Purpose

The *Event Logging* component maintains a reliable log of all community-related or member-related events.

E.30.2 Description

This *Event Logging* component plays an important role in establishing trust between a community member and the community platform. It documents all events (actions) which occur during the use of a community by members. Events comprise:

- Member related events: Actions performed by members, such as changing the current member location, uploading content, posting in forums, changing profile details, writing or receiving messages, etc. Other examples of events which are logged include which applications have accessed member profiles, what content has been submitted, which members have viewed that content and changes in privacy policies.
- Community related events: Events ranging from a new member joining the community or a sub-group, through to reporting technical or statistical events (e.g. number of members, average visiting time per user, reaction to particular advertisements, etc.)

Each member can decide which events are to be automatically communicated to other members. For example, uploading new pictures to a member's picture album could trigger a communication to all of his members of a sub-group or only to a smaller list of close friends.

Community related events benefit both members and the community provider. They provide information that helps manage provisioning, system availability and maintenance of the community, as well as indicate where to improve or adapt the services offered. They are also required to demonstrate that privacy policies are being respected.

The event log is available for members to inspect. Members can use this facility to verify that their profile data and content is being correctly managed, and to detect privacy breaches.

The *Event Logging* component collects event information from the other PICOS components. This information is archived to the secure (read-only) event log, where it is available for inspection, to prevent fraud.

Sometime it is not enough to simply monitor events. Events combine to form transactions, which can often reveal more about a community than individual events alone. The *Event Logging* component is able to associate events, based on its knowledge of the community, and thereby maintain a richer

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

record of the day-to-day use of the community. This can be of particular help when analysing the performance of services.

E.30.3 Dependencies

Components that this component calls	Purpose
None defined at present	

Components that call this component	Purpose
All components that give rise to event that affect the community.	

E.30.4 Drawing

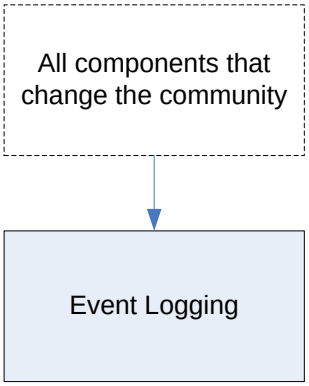


Figure 95 Event Logging

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

E.31 Event Reconstruction

T2 PICOSdistinguishing

PICOS Principle (PP): 1, 20, 23

PICOS Feature (PF): 1

E.31.1 Purpose

The *Event Reconstruction* component is responsible for assisting with the rebuilding of the community in the event of a catastrophic failure or should there be a need to create a duplicate community for investigative purposes.

E.31.2 Description

The *Event Reconstruction* component is concerned with the recovery of a system or of lost data. It also provides a means to gather evidence and test system functionality. Overall, event reconstruction creates greater member confidence.

Online communities are relied upon by millions of members to provide a reliable, always available resource. In reality, this is not the case for the Internet or web-based information, which is where these expectations are set. The average lifespan of a web page is 44 -75 days.

The PICOS community must be able to reconstruct itself in the event of failure. Website recreation utilities already exist[20], as do website and online services (Web services) that enable a website to be recreated reflecting its status at any point in history[21]. To a degree, it is possible to restore lost information by trawling the Web using one of the many search engines (e.g. Internet Archive, Google, Live Search, and Yahoo). However, despite the belief that 'no information is ever lost', reconstructing a community can be necessary and difficult.

The *Event Reconstruction* component works along side the *Event Logging* and *Audit* component to rebuild a community using details of transaction, events and archived data.

Retaining such extensive information obviously leads to concern about privacy. Access and operation of the *Event Reconstruction* component is thus tightly controlled.

[20] Frank McCown at Harding University created a tool called Warrick that helps the user to recover any lost website (or single web page) automatically (http://warrick.cs.odu.edu/).
[21] The 'wayback machine'.

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

E.31.3 Dependencies

Components that this component calls	Purpose
Event Logging	To gather information to facilitate the reconstruction.
Audit	To gather information to facilitate the reconstruction.

Components that call this component	Purpose
Service Selection	To gain access to Audit tools.

E.31.4 Drawing

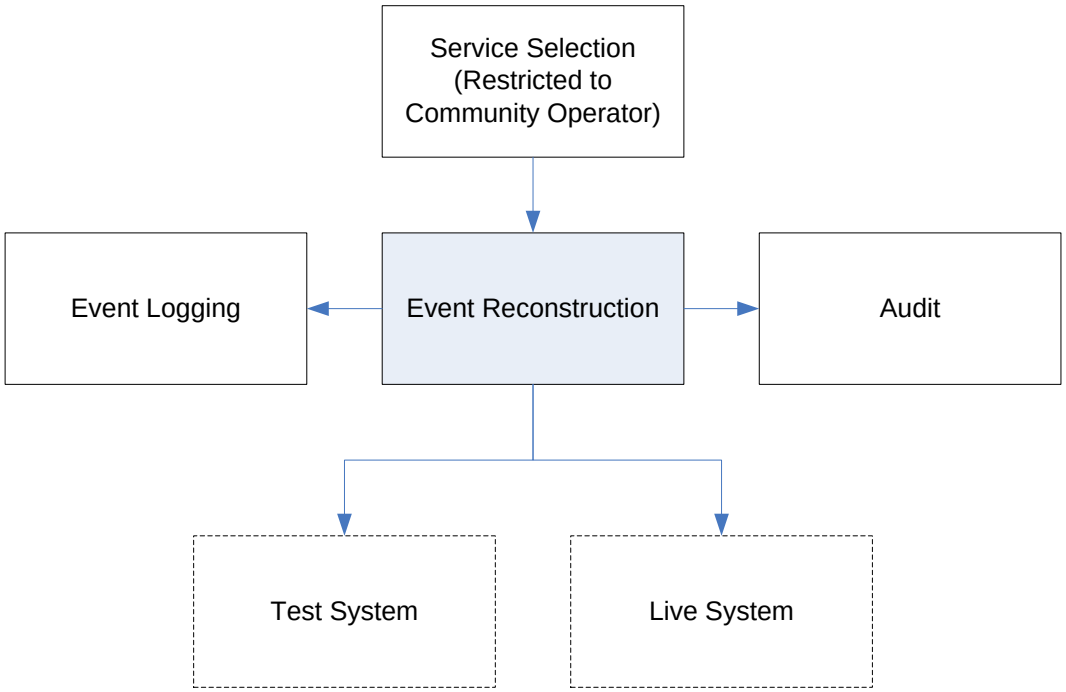


Figure 96 Event Reconstruction

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

E.32 Intrusion Detection

T1 PICOSenhancing

PICOS Principle (PP): 4

PICOS Feature (PF): 13

E.32.1 Purpose

The *Intrusion Detection* component is responsible for detecting attacks on the PICOS community.

E.32.2 Description

The *Intrusion Detection* component detects attempts to compromise the security of the PICOS system, with primary attention to the PICOS server. Security is usually understood in terms of achieving confidentiality, integrity/authenticity and availability of data and resources.

It is important to consider intrusion detection at various layers.

- Security of the network should be protected by firewalls and logs regularly analysed.
- Security of the operating system also plays an important role.

Intrusion detection is a complex task, and both of the above examples are beyond the scope of the PICOS project. The *Intrusion Detection* component in PICOS focuses on analysis of higher level events like authentication and registration attacks, events related to reputation management, attempts to access information protected with access control, and other unexpected behaviour (e.g. large number of posts, Spam, etc.). Thus, this component can be triggered by many of the other components, e.g. *Access Control*, *Communication Management* and *Service Selection components*, and probably *Content Sharing*, *Registration* and *Reputation Management* components.

A significant part of intrusion detection can be automated. However, it is very important to have the option to manually check log files in an easy manner and to verify the conclusions of the automated intrusion detection system.

Actions performed by the *Intrusion Detection* component include temporary and permanently blocking members and/or nodes, updating reputation and credential information (white/black lists).

It should also be noted that intrusion threats can come from insiders of a community, just as they come from outside. Their intent may be to subvert system integrity (information, reputation, logs, etc) or gain access to restricted data (private keys, bank accounts, VISA, PayPal, sensitive personal information, etc).

Tagging helps to identify data that is considered important/sensitive and thereby can facilitate the protection by focusing on the most sensitive data. For example private keys used for authentication must be strongly protected (e.g. hardware token, smart cards), because a breach could compromise the whole system.

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

It is important to recall that the law requests that the server stores sensitive information in a secure way to protect members' privacy from attackers.

E.32.3 Dependencies

Components that this component calls	Purpose
None defined at present	

Components that call this component	Purpose
Access Control	To trigger the intrusion detection response process.
Service Selection	To trigger the intrusion detection response process.
Communication Manager	To trigger the intrusion detection response process.

E.32.4 Drawing

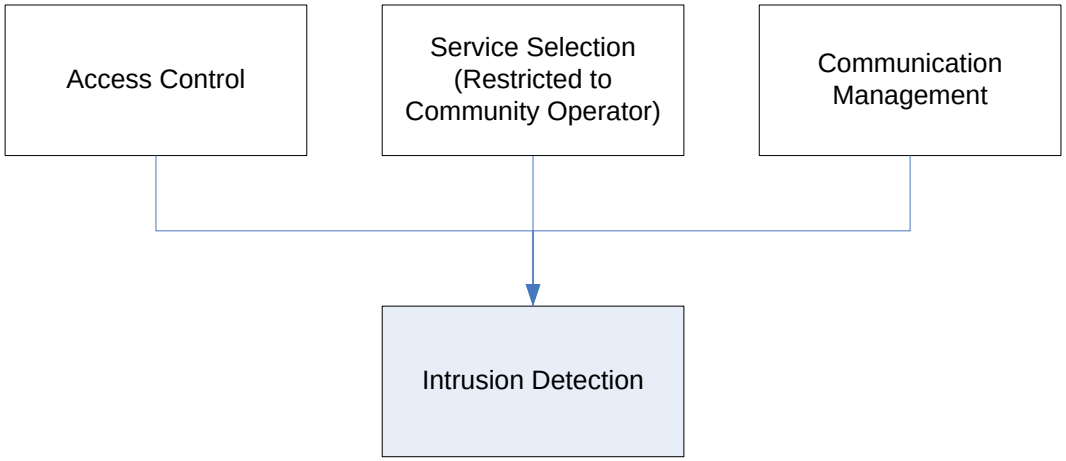


Figure 97 Intrusion Detection

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

E.33 Policy Management

PICOS D4.2 new/updated component

T2 PICOS distinguishing PICOS research

PICOS Principle (PP): 1, 3, 5,

PICOS Feature (PF): 2, 3, 11, 13

E.33.1 Purpose

The *Policy Management* component is responsible for policy that affects the whole community.

E.33.2 Description

Like many communities, policies play an important role in the PICOS community. Policies allow information to be communicated to members, demonstrating openness and transparency (and thus engendering trust), and allow broad 'default' operating practices to be established for large parts of the community.

Policy management falls into two main categories:

- Policy creation and sharing: This is where policies are recorded (edited) and made available to members. Often a standardised way of communicating policy will be used, and sometime this can be in machine readable form. Examples include W3C's P3P standard and IBM's EPAL proposal.
- Policy enforcement: A policy that establishes a standard, but which is not enforceable is arguably of little value. Enforcement can take many forms, but two popular ones are 1) proactive design of enforcement mechanisms and 2) reactive monitoring. Both approaches have their merits. At this stage in the project it is not possible to say which is preferable, or to explain how proactive enforcement would be achieved.

Policies remain a focus for the PICOS project and will be considered in more detail as the prototype evolves. Policies are also an area of research that PICOS might want to pursue.

Policy affects many aspects of a community. Two specific areas are authentication (and authentication method selection) and relationships with trusted third parties.

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

E.33.3 Dependencies

Components that this component calls	Purpose
Authentication Selector Method	To establish a community-wide set of approved authentication methods.
TTP Management	Where the chosen authentication method required the services of a Trusted Third Party (TTP), e.g. where an authentication token was issued by another community.

Components that call this component	Purpose
Service Selection	To administer community-wide policies.

E.33.4 Drawing

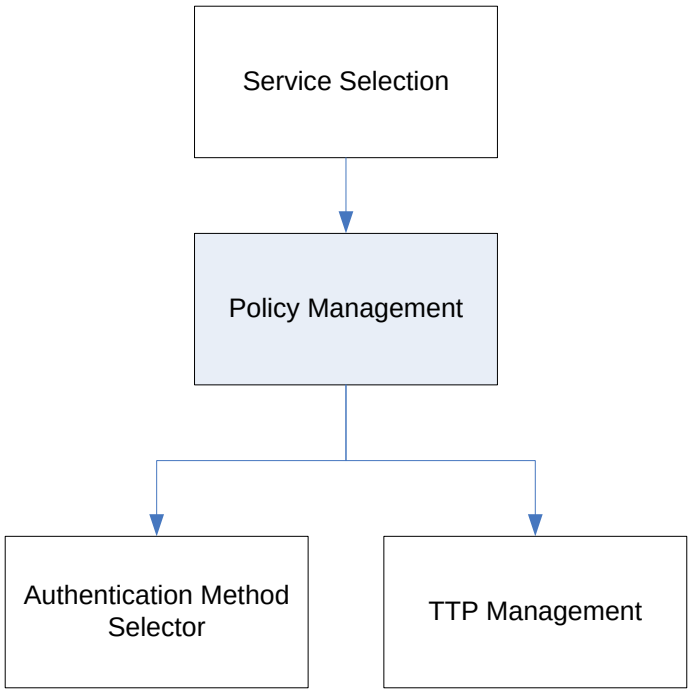


Figure 98 Policy Management

The Policy Manager functionality is extended for supporting to attach rules to the entities : Contacts list and Privates Sites.

The first case, privacy rules attached to Contacts is needed for allowing/disallowing to have access to the Contacts list of that Contact. This means that when one user want to authorize to see his Contact

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

list then he must go to Privacy Manager component and create a specific rule for that (for instance something like “I allow to see my Contacts list to Everybody”), and afterwards everybody will have access to his Contact list.

The other Policy Manager extension is for supporting to attach privacy rules to the Private Sites. One Private Site is defined like GPS coordinates plus radius parameter. Once the private area is defined, user could go to the Policy Manager and attach a privacy rule to it (for instance something like “these Contacts can see my location information if I am close to this Private Site with this precision”

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

E.34 Authentication Method Selection

T2 PICOSenhancing

PICOS Principle (PP): 17, 18

PICOS Feature (PF): 3

E.34.1 Purpose

The *Authentication Method Selection* component enables the selection of authentication method.

E.34.2 Description

Several authentication methods will be supported by the PICOS community. Exact details are not yet available, and will depend on the capabilities of the client device, but could include password, biometric, token and credential. The choice of which to use depends on the situation and context, and on the sensitivity of the action being performed. For highly sensitive information or actions, strong authentication is preferred.

The *Authentication Method Selection* component responds to the request from the *Access Control* component and the *Authentication* component, and for a given authentication method. The choice will be decided through community policy (*Policy Management* component), member profile (*Profile Management* component) and member preferences (*Data Minimisation* component and *Privacy Advisor* component), all under the direction of the *Access Control* component.

Where authentication takes place at the client, it is possible that a local version of this component will be required, i.e. where the *Access Control*, *Authentication* and possibly the *Authorisation* component are located at the client.

E.34.3 Dependencies

Components that this component calls	Purpose
Policy Management	To identity the preferred method(s) of authentication for the community as a whole.
Profile Management	To identity the preferred method(s) of authentication of the member.
Privacy Advisor	Where the member has a choice, the Privacy Advisor helps to select the method that best achieves data minimisation.

Components that call this component	Purpose
Authentication	To indicate to the member the preferred method(s) of

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

	authentication, having been triggered by the *Access Control* component.

E.34.4 Drawing

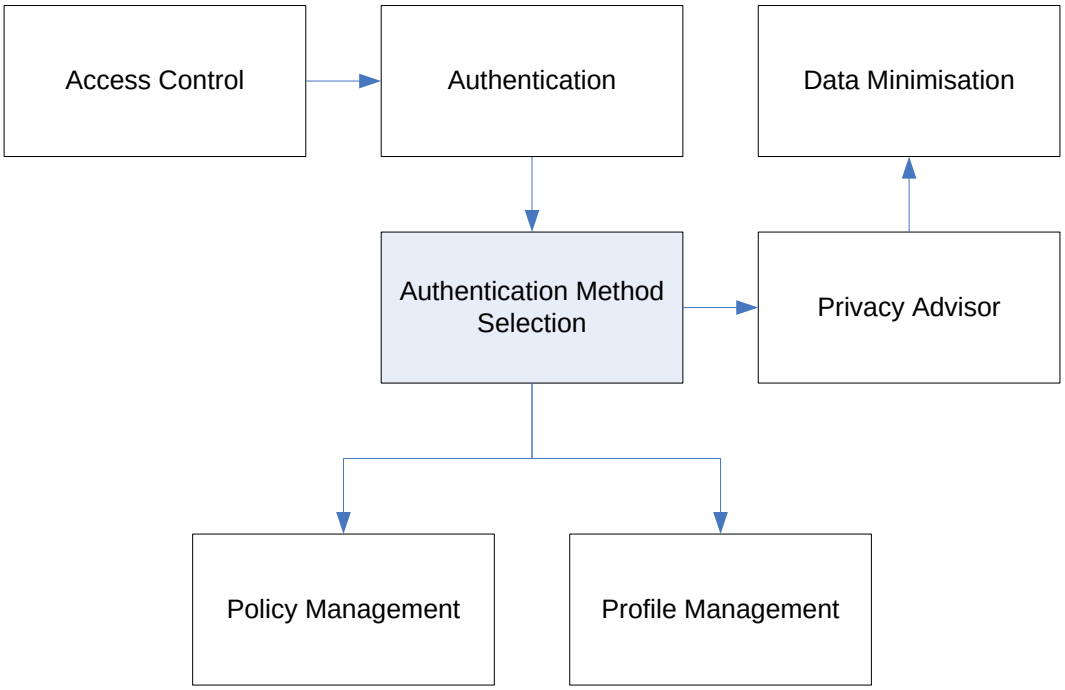


Figure 99 Authentication Method Selection

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

E.35 Consent Management

T2 PICOSdistinguishing

PICOS Principle (PP): 2, 3, 4

PICOS Feature (PF): 2, 10

E.35.1 Purpose

The *Consent Management* component allows members to grant consent for their personal information to be used in the way members wish.

E.35.2 Description

The *Consent Management* component plays an important role in both privacy management and trust management. It stores and enforces user-defined policies with respect to the sharing of members' profile information (and other member data) with other members and with external services. It indicates if the member gave consent for this data to be shared with others and, if so, what terms and conditions apply.

The *Consent Management* component also allows member to modify or withdraw their consent, and it invokes the community-specific procedures that are applied when consent is withdrawn, noting that different communities may interpret consent changes in different ways, e.g. deletion, change to access rights which restrict access to certain roles only. The latter involves the *Policy Management* component.

E.35.3 Dependencies

Components that this component calls	Purpose
Policy Management	To determine community policy on managing member information.
Profile Management	To determine member preferences on sharing personal information.

Components that call this component	Purpose
Content Sharing	To respect member preferences when sharing personal information.
External Services Delivery	To check consent before sharing information with an external service provider.
Social Presence	To take into account member current status before sharing

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

	personal information.

E.35.4 Drawing

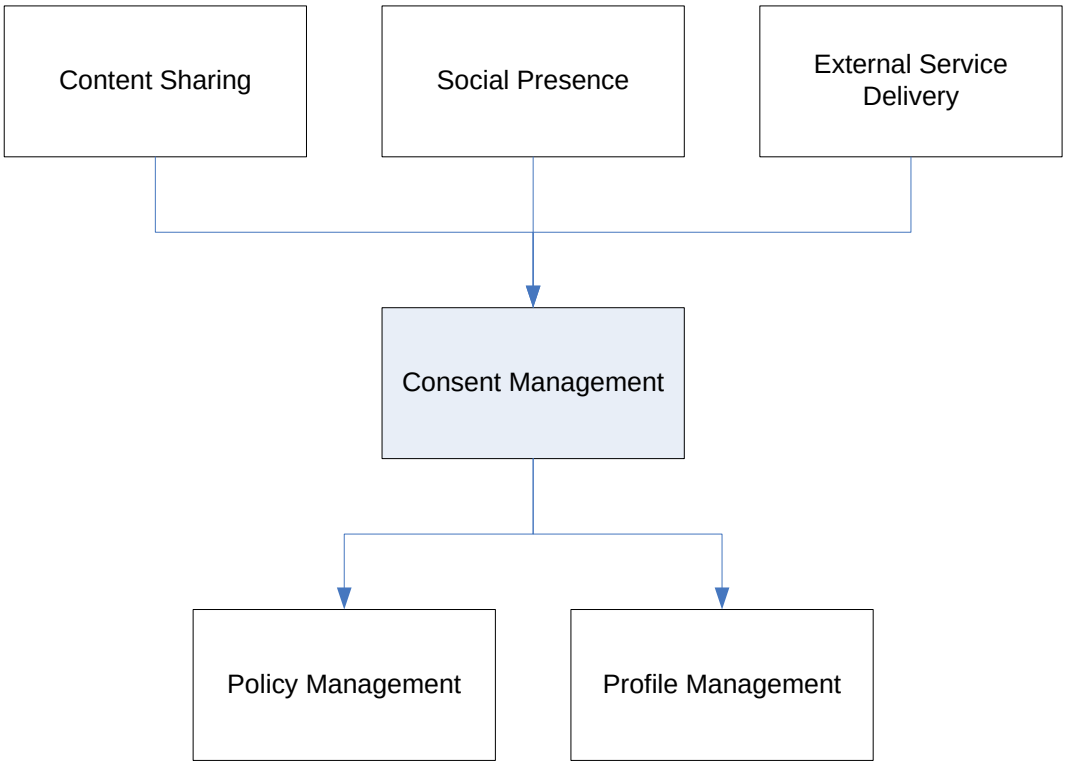


Figure 100 Consent Management

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

E.36 Cryptography / Key Management

T2 PICOSenhancing

PICOS Principle (PP): 1, 4, 8, 9, 17

PICOS Feature (PF): 1, 3, 10, 15

E.36.1 Purpose

The *Cryptography / Key Management* component implements cryptography and key management mechanisms and services.

E.36.2 Description

The *Cryptography / Key Management* component provides support for symmetric and asymmetric public key cryptography, offering confidentiality and integrity mechanisms. The mechanisms supported fall into four categories:

- Confidentiality: RSA encryption/decryption and signatures
- Integrity: Hash, AES encryption/decryption, etc
- Non-Repudiation: DSA signatures, Schnorr signatures, ElGamal signatures & encryption
- Traceability: Group, FTMGS signatures, etc ...

Key management is an important part of any cryptography scheme. Keys need to be created, stored and generally managed securely. Retrieving the correct key to use with a mechanism for a particular purpose is also something that needs to be handled with care, especially where keys are transferred from one domain (e.g. server) to another (e.g. client) before use.

Keys are stored by the *Secure Repository* component, which may be implemented on either the server or client, or both.

Access to keys is indirectly controlled by the *Access Control* component, and access will be dependent on valid authorisation (*Authorisation* component). Access is granted where authentication is satisfied and the role is appropriate.

Many components may require access to this component, but the main components are *Network Security*, *Anonymisation*, *Secure Repository*, and *Authentication*.

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

E.36.3 Dependencies

Components that this component calls	Purpose
Anonymisation	To generate keys.
Authentication	To support mutual authentication and credential authentication methods.
Network Security	To access algorithms/keys required for network confidentiality and integrity.
Secure Repository	When preparing sensitive information for storage.

Components that call this component	Purpose
Secure Repository	To store/retrieve keys.

E.36.4 Drawing

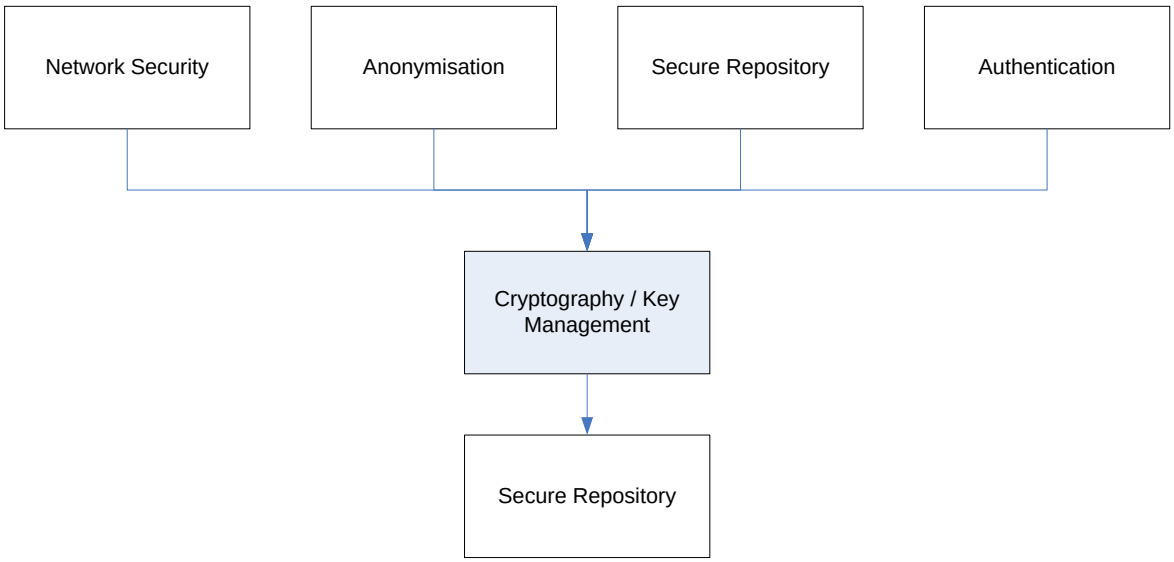


Figure 101 Cryptography /Key Management

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

E.37 Delegation

T2 PICOSenhancing

PICOS Principle (PP): 2, 23

PICOS Feature (PF): 3, 7, 15

E.37.1 Purpose

The *Delegation* component allows members to transfer privileges between partial identities which may (or may not) belong to different members (with different root identities).

E.37.2 Description

Using the *Delegation* component, members can delegate privileges that come with their partial identity to other partial identities or to other members' partial identities. The reason they might want to do this is to allow another member to perform an action with an asset that they considered personal. Whenever delegation is invoked, all actions are logged (by the Event logging component) so that it is clear what events have taken place and by whom.

Typically, delegation will expire on completion of an action or after a predetermined time. The member to whom privileges are delegated cannot influence the privileges originally assigned to the delegating member, but it is possible that the reputation of the delegating member (and the delegated member) might be affected by events that occur while delegation is active.

Delegation is only possible with the consent of both parties (*Consent Management* component), and if accepted will affect the profiles of one (and possible both) members (*Profile Management* component, *Privilege Management* component). It is also appropriate that both members are formally notified of the change (*Notification* component).

Delegation can takes two forms:

- Delegation of authentication: Assuming that a credential is used to authenticate a member to a community, that a credential can be delegated to another system or community, pass-through authentication is possible. This is when a member accesses one community, which then automatically signs the member into another community. This is an example of Single Sign-On (SSO), e.g. Open Id.
- Delegation of authorisation: A member can delegate their access rights to another member, so that the other member can act on the delegating member's behalf.

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

E.37.3 Dependencies

Components that this component calls	Purpose
Consent Management	To check the consent of both partied involved in the delegation
Notification	To notify the delegated member that delegation has taken place, e.g. if delegation occurs automatically or because of prior agreement between the two parties.
Privilege Management	To update the privilege of the delegated member.
Profile Management	To update the profile of the delegated and delegating member.

Components that call this component[22]	Purpose
Service Selection	To trigger delegation.

E.37.4 Drawing

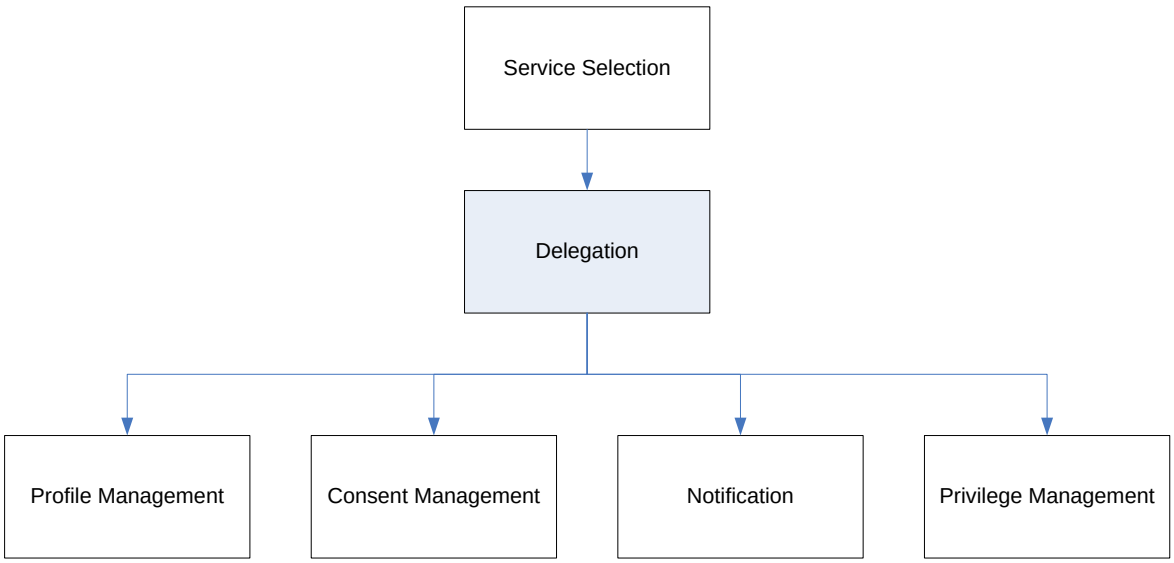


Figure 102 Delegation

[22] The dependencies with other components of PICOS architecture will be basically the first point to access to the network operator (the SIP Proxy or P-CSCF in case an IMS network is available).

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

E.38 Identity Lifecycle Management

T_1 PICOS$_{enhancing}$

PICOS Principle (PP): 11, 17, 18

PICOS Feature (PF): 1, 3, 4

E.38.1 Purpose

The *Identity Lifecycle Management* component manages all aspects of identity in the community.

E.38.2 Description[23]

The *Identity Lifecycle Management* component interacts with the main components that support the lifecycle of a member, namely the *Registration*, *Partial Identity Management*, *Privilege Management*, *Delegation* and *Revocation* components. It also accesses the *Policy Management* component to determine community policy.

Identities experience a well-defined lifecycle in PICOS communities (from enrolment of members until their termination). The management of such a lifecycle is a core feature of any identity management solution, whether centralised, user-centric, federated or a combination of several models. Essentially, the Lifecycle Management presents a framework which ensures that identity information is accurately maintained in a context, in accordance with applicable policies, standards and regulations.

Lifecycle Management results in a level of assurance[24] which in turn results in an acceptable level of risk for the individual and the community. In practice, the level of assurance will vary depending on various factors, e.g. personal, business, legal, regulatory, internal policies, etc.

Identity Management consists of:

- Registration
- Creation
- Modification
- Delegation
- Revocation

Identities follow a lifecycle, e.g. established, modified, suspended, terminated, archived and transferred. An identity is typically only valid for a period of time (i.e. has a start/end date) and its existence may be dependent on context. The identity of an entity may persist after the entity ceases to

[23] See ISO/IEC JTC 1/SC 27 WG5 N7109 "A framework for Identity Management" pp. 22-26

[24] It may benefit all organizations and individuals in multiple contexts to provide a certain assurance level that an identity is not compromised or will not be repudiated. The assurance level required is determined by the risk of not effectively distinguishing entities with the means of the context.

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

exist when entity information still needs to be managed. The possible states of an identity are the following:

- Not Established: the identity of an entity is unrecognised in a given context. In some cases the entity exists, and in others the entity does not exist.
- Established: the identity of an entity is recognized in the context but the entity is not yet able to interact with other entities in the context.
- Activated: the identity of an entity is recognized in the context and the entity is able to interact with other entities in the context according to the purposes of the context.
- Suspended: the identity of an entity is recognized in the context. However, the entity is no longer able to interact with other entities in the context.
- Terminated: an entity is no longer recognized in a context.
- Archived: an entity is no longer recognized in a context but records may be required to remain available to determine whether or not an entity has in the past been recognized in a context with a particular identity.

These states and the sequences of events that can cause transitions between them are depicted below:

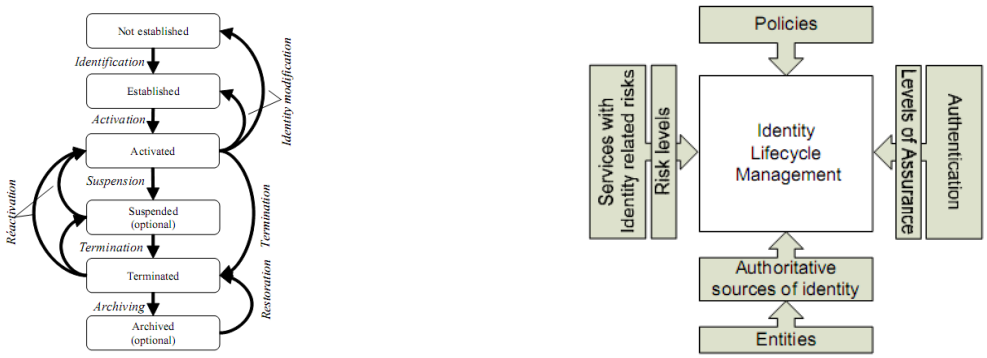


Figure 103 States in an identity lifecycle

A useful description of how identity lifecycle management is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 1: Registration
- PICOS Use Case 2: Accessing the community
- PICOS Use Case 4: Multiple Partial Identities
- PICOS Use Case 5: Revocation

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

E.38.3 Dependencies

Components that this component calls	Purpose
Delegation	To delegate authority to another partial identity.
Partial Identity Management	To monitor the creation of partial identities.
Policy Management	To manage policies relating to partial identities.
Privilege Management	To set/modify privileges for partial identities.
Registration	To register new root identity (member) and prepare for the creation of a partial identity.
Revocation	To revoke a partial identity or a root identity.

Components that call this component	Purpose
None. (Internal community function)	

E.38.4 Drawing

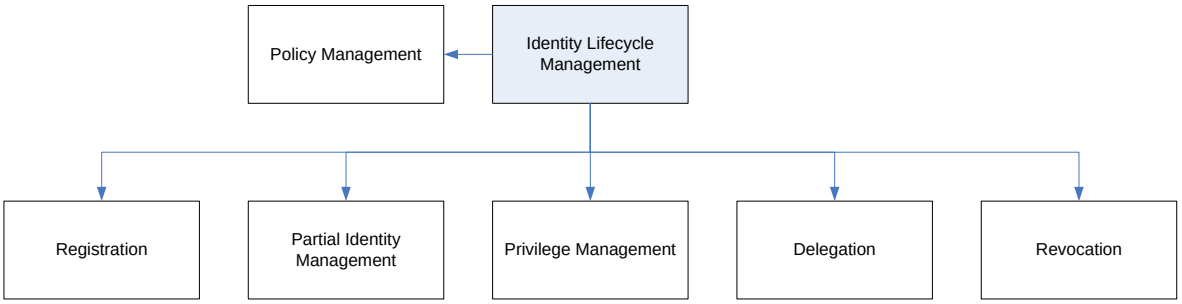


Figure 104 Identity Lifecycle Management

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

E.39 Privilege Management

T2 PICOSenhancing

PICOS Principle (PP): 3

PICOS Feature (PF): 2, 3

E.39.1 Purpose

The *Privilege Management* component enables the setting and modification of member privileges, typically by the community operator.

E.39.2 Description

Every member is assigned privileges which grant or deny access to community resources. Privileges are established using the *Privilege Management* component at the time the member is enrolled, triggered by the *Registration* component. Members who have multiple identities (partial identities) will have multiple sets of privileges (privilege sets), but only one set of privileges is assigned to each partial identity.

In a typical computer operating system, users are assigned to groups. In a PICOS community, groups are represented by sub-communities. Just as with groups, sub-communities can only be accessed by members who possess the prerequisite privilege.

Partial identities can inherit the privileges of a root identity, or of another partial identity using the *Delegation* component. Delegation is also an area where privileges will change (semi-) automatically.

Another way to consider privilege sets is as definitions of roles. A member may be asked to carry out a specific function on behalf of the community. To perform these functions the member will need an enhanced set of privileges. Thus a privilege set can be assigned to a role, e.g. manager, auditor.

The *Privilege Management* component manages privileges, i.e. it facilitates the creation, modification and assignment of a privilege set to a partial identity.

Privileges are treated just like any other personal information. Following the model of data minimisation that PICOS adopts, only those privileges necessary to perform a function have to be declared. In addition, the rights demonstrated by privileges can be demonstrated in an anonymising (or privacy friendly) way using zero knowledge proofs (ZKP).

The management of privileges makes the assumption that the identification of entities is guaranteed[25]. Managing privileges involves four main activities:

- Definition of privileges and the privilege set

[25] The authentication of 'proper owners' in PICOS is flexible and accounts for different levels of authentication depending on context, policies, etc. (i.e. users could also be pseudonymously or anonymously authenticated to the community).

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

- Validation of authorisation to assign privileges to entities, ensuring that privileges are securely granted to entities based on conditional attributes specific to each community, roles and tasks and possibly approvals from different actors in some cases
- Provisioning of authorised privileges to entities, so that access to community information and resources in based on a trusted identity/entity
- Control of provisioned privileges when accessing resources, so that the manner in which the controls are operated determines how privileges must be defined and the basis of such controls may be heterogeneous, i.e. based on given mandates, role assignment, contextual constraints and conditions, and possibly automated authorisations

When accessing resources with privilege thresholds, other conditions may also need to be fulfilled, e.g. rules based on context or scenario. Reference to the *Policy Management* component, the *Social Presence* component and the Reputation Management component may be required.

Members are able to view their privileges via their personal profile using the *Profile Management* component.

Privileges may also be adjusted (promoted/demoted) according to reputation, feedback or a change in role.

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

E.39.3 Dependencies

Components that this component calls	Purpose
None defined at present	

Components that call this component	Purpose
Delegation	To retrieve and transfer privileges to a partial identity. Note: Trigged by *Service Selection* component
Profile Management	To set/modify member privileges.
Registration	To assign privileges to a new member.

E.39.4 Drawing

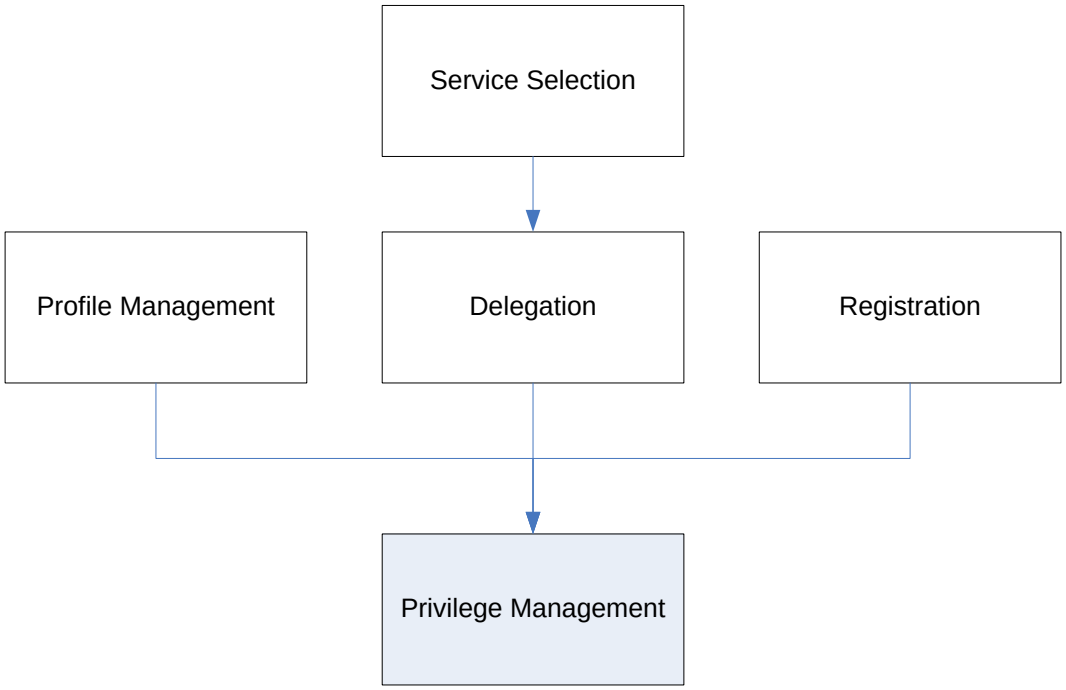


Figure 105 Delegation

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

E.40 Profile Management

T2 PICOSdistinguishing

PICOS Principle (PP): 4, 23

PICOS Feature (PF): 4, 8

E.40.1 Purpose

The *Profile Management* component provides access to the profile of an entity.

E.40.2 Description

Every partial identity possesses a personal profile that contains partly public and partly private information. Note that partial identities apply to a member, but also to other entities within the community that need to be uniquely identified, e.g. external services.

The personal profile describes each member's attributes, interests, general preferences and privacy preferences. The profile also contains a dynamic indication of a member's availability to interact with other members. Members can choose what information maintained by the community is revealed to others, e.g. their diary. Willingness to receive advertising is also recorded in the profile. This is managed by the *Consent Management* component.

Members can modify their personal profiles at any time using the *Profile Management* component, but they cannot alter settings that are established by the community, e.g. role, status, sub-community membership, etc. Information can be added to or removed from a profile, so long as the result is not misleading to other members.

A profile may also carry social presence (status) information, which is conditionally visible to other members and the community operator. For other members, social presence provides a real-time indication of the availability of the member. For the community operator, social presence indicates the status of the member's membership, e.g. pending, expired, account locked, membership 'paid up', roles, sub-communities owned, duration of membership, etc.

Privacy preferences enable members to specify the level of privacy that applies to all or part of the personal information that they share with others. Privacy preference can apply to individual data items or to a set of data items which together profile the member in a particular way. Privacy preferences are interpreted by the community and acted upon, thus fulfilling the privacy wishes of the member. The ability of the system to enforce preferences in a given situation/scenario (or context) is a key factor in establishing member trust and confidence.

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

E.40.3 Dependencies

Components that this component calls	Purpose
None defined at present	

Components that call this component	Purpose
Authorisation	To check the privacy preferences in the profile.
Consent Management	To update the privacy preferences in the profile.
Content Sharing	To check the privacy preferences in the profile.
Privacy Advisor	To check the privacy preferences in the profile.
Registration	To create the profile.
Service Selection	To access the profile management service.

E.40.4 Drawing

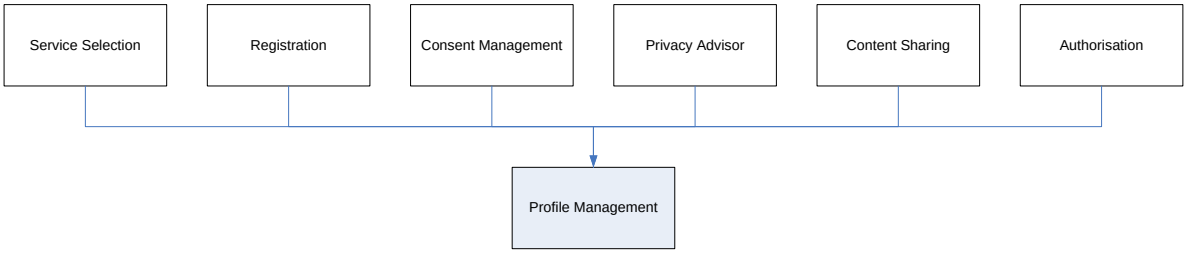


Figure 106 Profile Management

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

E.41 Registration

T2 PICOSenhancing

PICOS Principle (PP): 17

PICOS Feature (PF): 3

E.41.1 Purpose

The *Registration* component handles new member registration.

E.41.2 Description

The *Registration* component allows an individual to acquire membership of a community for a period of time, and enjoy the benefits associated with membership. Registration involves creating a unique root identity and one or more associated partial identities, and acquiring the ability to authenticate that identity to the community. It also involves agreeing to the terms and conditions of the community.

For a PICOS community, registration also involves a member stating privacy preferences (these processes are handled by separate components) and being assigned privileges.

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. Registration occurs prior to authentication and authorisation. In a simple model, members register directly with a community, much like an individual registers with a web-based online service.

In a mobile setting, it is possible that the individual has already authenticated themselves to the mobile operator (e.g. T-Mobile) and in theory does not need to authenticate or even register with the community, although in practice (and in the case of a PICOS community) members will be expected to register with the community directly.

Despite the convenience of having just one point of authentication, the community must always satisfy itself that only legitimate members can gain access to its resources. For this reason, the *Access Control* component will always be the first point of contact for new and existing members, and will direct them to the *Registration* component. It is at the time of registration that new members are allocated privileges and resources.

When a member subsequently attempts to access the community, they will be asked for their identity and challenged in order to authenticate. Once access is granted, privileges are retrieved and other members are able to check this member's status.

Example: In the figure below P-CSCF is an authentication point provided by the mobile operator, here using a SIP[26] protocol[27][28].

[26] SIP is popular with 3GPP (Third Generation Partnership Project)

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

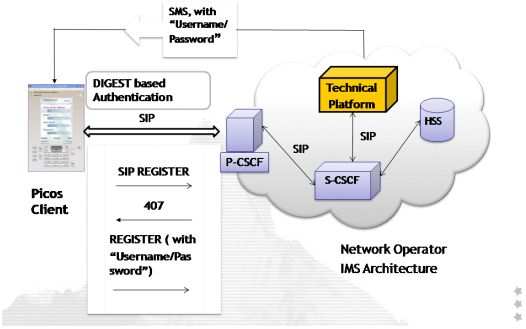


Figure 107 Example of Registration implementation using SIP

A useful description of how registration is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 1: Registration
- PICOS Use Case 2: Accessing the community
- PICOS Use Case 4: Multiple Partial Identities

[27] All RFC 3261 compliant user agent (SIP client application) support Digest Authentication, which uses a shared secret, as a means for authentication to a SIP Proxy. The registration allows a user agent to express that it is an appropriate entity to which requests should be sent for a particular SIP address (SIP URI).

[28] SIP traffic is initiated by a registration that is challenged by the P-CSCF using Digest based authentication. The Technical Platform relies on the S-CSCF to manage the access control and handle the SIP P-Asserted identity header so that each SIP component can rely on the SIP user identity (public SIP URI) behind the S-CSCF.

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

E.41.3 Dependencies

Components that this component calls	Purpose
Partial Identity Management	To create the initial partial identity.
Profile Management	To set root identity profile.

Components that call this component	Purpose
Identity Lifecycle Management	To trigger the registration process.

E.41.4 Drawing

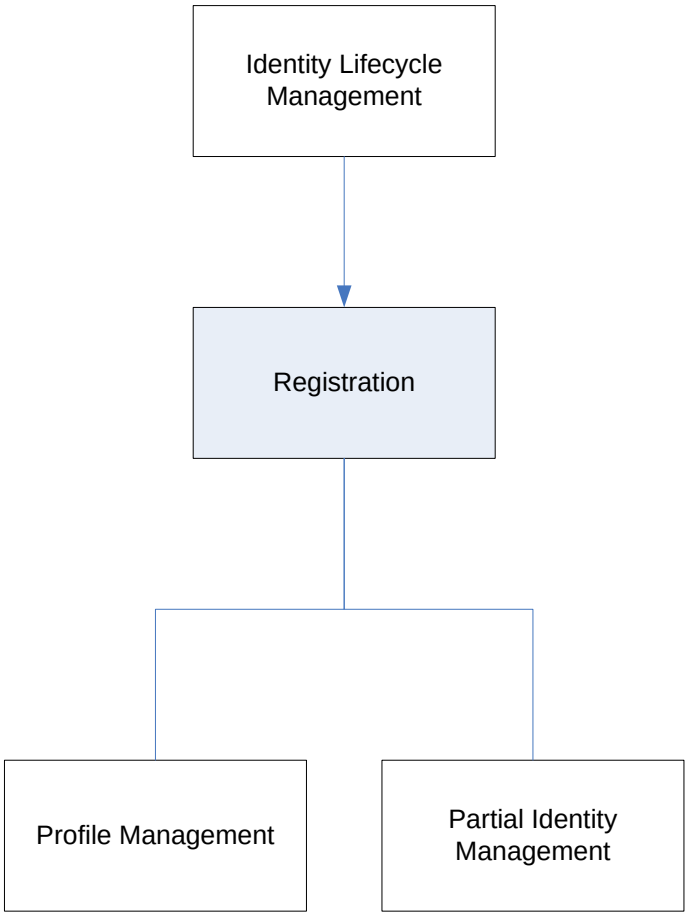


Figure 108 Registration

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

E.42 Revocation

T2 PICOSenhancing

PICOS Principle (PP): 2, 12, 23

PICOS Feature (PF): 2, 10, 15

E.42.1 Purpose

The *Revocation* component is responsible for terminating a member's access to the community.

E.42.2 Description

The *Revocation* component is called whenever a member wishes to leave the community (or is asked to leave the community), or when a member wants to terminate a partial identity.

When a member wishes to leave (resign) from a community they will most likely leave behind information that must be retained and protected. It is unlikely that this information can simply be deleted from the community (or even removed) since it may be shared or required for legal purposes. Regardless, it could contain personal information (personal profile, pictures, personal messages and other personal assets) that continues to need protection. Revocation requests the *Anonymisation* component to pseudonymise (in a reversible way, such as encryption) all references in all databases to the identity of this individual, and then after a second period of time, all these reversible pseudonyms are converted to irreversible pseudonyms (for example a hash of the previous pseudonym). Additionally, after a period of time, all sensitive data belonging to this individual must be erased.

Revocation is not concerned with data that has been transferred (e.g. as an attachment to a personal message) to another member or group of members, as this data is considered to be outside the original member's control.

Revocation can only be initiated by the community operator. However, it is possible for a member to revoke partial identities (which, incidentally are always linked to the creating root identity) but all personal assets are transfer to the creating identity, and the legal requirement to retain information still applies.

Revocation is recorded as a community event, thus it is possible to recreate an identity if necessary.

Revocation also influences membership status, and forces authentication information to be destroyed (to prevent further access). Reputation information may also need to change as a result of the member leaving the community.

A useful description of how revocation is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 3: Revocation

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

E.42.3 Dependencies

Components that this component calls	Purpose
Partial Identity Management	To revoke a partial identity.
Profile Management	To revoke a root identity profile.

Components that call this component	Purpose
Identity Lifecycle Management	To activate the revocation process.

E.42.4 Drawing

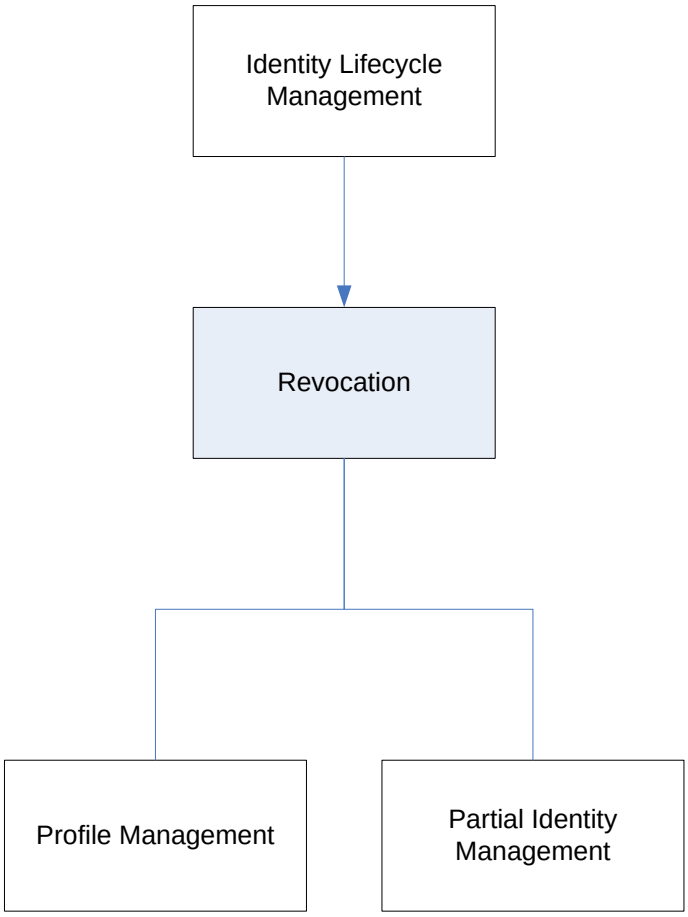


Figure 109 Revocation

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

E.43 Sub-community Management

PICOS D4.2 new/updated component

T1 PICOS enhancing

PICOS Principle (PP): 19

PICOS Feature (PF): 7, 10

E.43.1 Purpose

The *Sub-community Management* component is responsible for managing sub-communities created by a partial identity.

E.43.2 Description

The *Sub-community Management* component addresses how members interact with external and sub-communities. Every partial identity is a member of the PICOS community or sub-community.

External communities (inter-community) and sub-communities (intra-community) may initially appear very different, but the issues of trust and privacy that each experience are very similar. They concern access rights, which are derived from a member's profile and privileges, assigned when they registered with the community.

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. In the case of a sub-community, in response to the request from the member to create a sub-community, the *Sub-community Management* component will build the community and assign ownership to the member. It will set up all monitoring and any other services that the sub community requests. Since an external community already exists, there is no need to create anything, but the monitoring process (which occurs within the local community) will need to be initiated.

Sub-communities maintain a list of members who can access the sub-community (in its profile) using the *Profile Management* component.

A useful description of how sub-community management is employed in PICOS can be found in sub-section 13 in:

- PICOS Use Case 9: Sub-community

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

E.43.3 Dependencies

Components that this component calls	Purpose
Profile Management	To set up and manage the profile of a sub-community.

Components that call this component	Purpose
Service Selection	To administer sub-communities.

E.43.4 Drawing

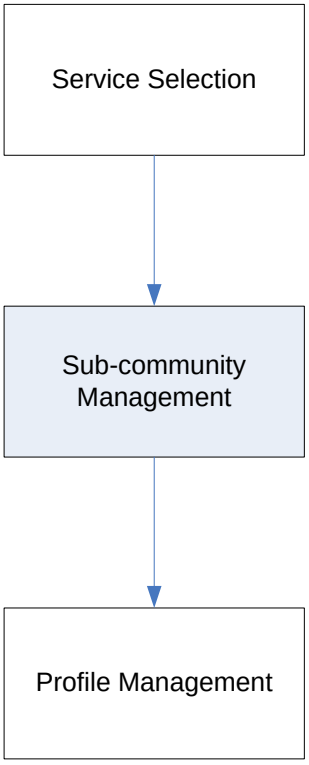


Figure 110 Sub-community Management

The same additional functionality added in Public Communities Threads, will be added in Sub-Communities Threads. This means that both features: attach privacy rules to forum Threads and subscribe to new available content, will be supported by Sub-communities as well.

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

E.44 Content Sharing

T_2 | PICOS$_{enhancing}$ | PICOS$_{distinguishing}$

PICOS Principle (PP): 4

PICOS Feature (PF): 2

E.44.1 Purpose

The *Content Sharing* component is responsible for making imported content available to members.

E.44.2 Description

The *Content Sharing* component contributes, administers, manipulates and communicates content imported by one member to other members. The contributing member can control who can see the content, using the tagging and privileges, and indirectly by role and context. Members can be notified that new content is available using the *Notification* component.

Content sharing is triggered automatically when a member imports content, using the *Importer/Exporter* component, or on demand using the *Service Selection* component.

Content is shared under a partial identity of the member to help maintain privacy.

The function of the *Content Sharing* component permit:

- Contribution
- Upload content elements
- Publishing content on the personal profile (e.g. pictures in a picture album)
- Administration
- Managing content: Organising personal messages; Organising picture and video albums; Deletion of content elements
- Setting and managing policies for restriction of the access to content by other users.
- Manipulation
- Editing content elements
- Editing tags for content elements
- Communication
- Publishing content on the personal profile
- Forwarding content elements to other users
- Attaching content elements to messages, forum posts, etc.

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

Content is shared with other members in one of three ways:

- Member to member
- Member to sub-community
- Member to community

Other possibilities exist, e.g. community to community, and member to component, i.e. reputation, which are not discussed further.

A useful description of how content sharing operated in PICOS can be found in sub-section 13 in:

- PICOS Use Case 7: Content Sharing

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

E.44.3 Dependencies

Components that this component calls	Purpose
Notification	To notify other members that new (or changed) content is available.
Privilege Management	To control which members can access content.
Profile Management	To check if a member wishes to be identified when sharing content.

Components that call this component	Purpose
Importer/Exporter	To share imported content.
Service Selection	To share content.

E.44.4 Drawing

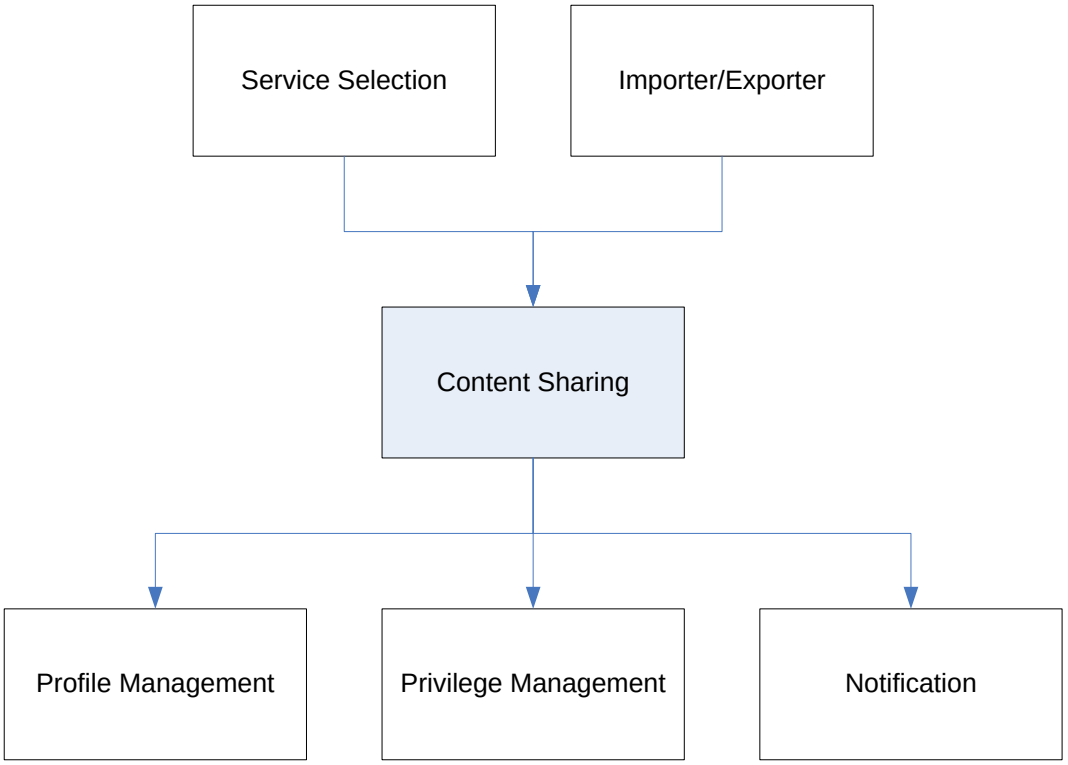


Figure 111 Content Sharing

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

E.45 Data Minimisation

T2 PICOSdistinguishing PICOSresearch

PICOS Principle (PP): 3, 8

PICOS Feature (PF): 2

E.45.1 Purpose

The *Data Minimisation* component minimises the unnecessary exposure of member personal information.

E.45.2 Description

Data minimisation is one of the main building blocks on a PICOS community. The objective is for a member to never be required to provide more personal information than is absolutely necessary to gain access to a service. Data minimisation is the primary method for providing privacy and protecting identities[29].

Strictly speaking, data minimisation minimises the collection of data regardless of its purpose (going beyond the "Collection Limitation" Privacy Principle[30]). Additionally data may be requested if it is clear to the individual that it is optional and there is clear justification for collecting it, or when collection is an obvious and agreed benefit to the member.

PICOS uses the *Data Minimisation* component to support members in minimising the information they provide, following the principle of 'minimal disclosure of information'[31]. Thus, data management is a core feature of identity management within PICOS, since data minimisation ensures that data is accurately managed in a context, in accordance with applicable policies, standards and regulations.

In the scope of community operations, only data relevant and necessary will be requested and transmitted, except for data that members consciously and willingly choose to share with each other and/or the community.

The design of data processing systems considers non-identifiable interactions and transactions by default and, wherever possible, identification, observation and linking of personally identifiable information is minimised.

Often members are not aware which kind of information has to be provided in order to use a certain service. Consequently they often either give too much information or refuse to use the services. By providing guidance to member, PICOS helps member understand their options in the context of their own actions. Furthermore, the system supports members' right to be informed before the processing of data starts and allows rectifying, erasing, or blocking their data. On the other hand, community

[29] See PICOS D2.3 Contextual Framework, p.29

[30] Privacy principles represent a basic set of overall commonalities in the fundamental privacy requirements to prevent the misuse of personally identifiable information when processing it in information and communication technology. See ISO/IEC JTC 1/SC 27 N56734 "A Privacy Framework" p.16.

[31] See PICOS D2.4 Requirements, section 3.1.2, p.56.

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

providers tend to collect data ahead e.g., for statistical or advertising reasons. Therefore, it is necessary to constrain them to collect only data that is needed to provide respective information or services.

In addition, members have very different values, and some member may want to publish/share more personal data than others, whether sharing information with other members, with the community provider (e.g. for using specific community services) or with third parties (e.g. for marketing purposes). For this reason PICOS provides members with the option to manage their own level of data minimisation, e.g. giving them the option to choose what information they share and with whom[32], while showing in an easily understood manner how their information will be held, taking into account the context in which information will be handled.

Data minimisation can be implemented in the client side and/or the server.

[32] Users may also choose to make use of anonymisation / pseudonymisation services and other mechanisms to further protect their personal information, even after deciding to share more personal data (see section 7 of ISO/IEC JTC 1/SC 27 N6736 "A Privacy Reference Architecture"

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

E.45.3 Dependencies

Components that this component calls	Purpose
None define at present	

Components that call this component	Purpose
External Service Delivery	To minimise information exposed.
Identity Translator	To minimise information exposed.
Privacy Advisor	To determine options to minimise information exposed.

E.45.4 Drawing

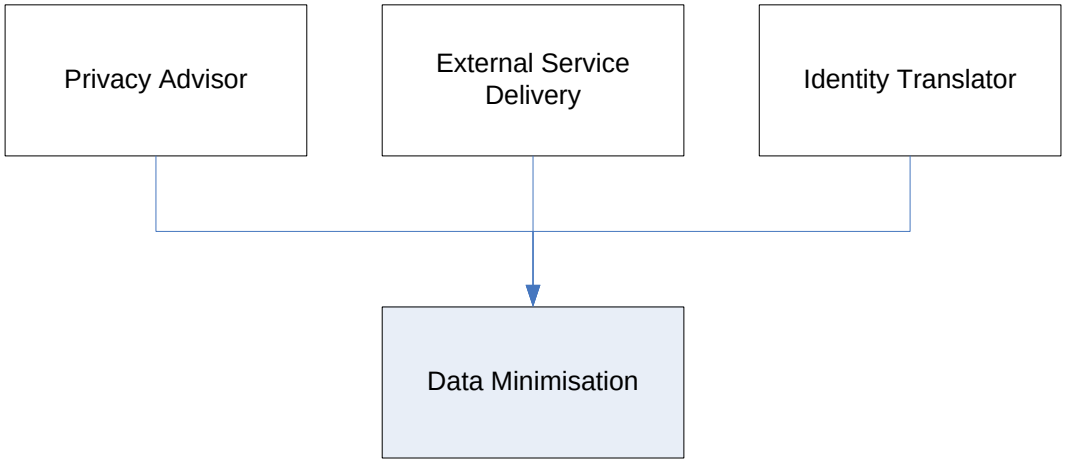


Figure 112 Data Minimisation

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

E.46 DRM

T2 PICOSenhancing

PICOS Principle (PP): 2, 10, 23

PICOS Feature (PF): 2

E.46.1 Purpose

The *DRM* component ensures that content is used in accordance with the terms and conditions of the owner.

E.46.2 Description

The *DRM* component is associated with the *Access Control* component. It ensures that content on the community portal – whether professional content or user-generated content - is accessed (viewed, downloaded, shared) in accordance with the terms & conditions defined by the content owner or community operator.

If the content owner or community operator specifies certain usage terms (e.g. which devices can be used to view content, who can the content be shared with, how many times can the content be accessed, etc), this function ensures that those policies are respected.

Although it is possible that PICOS will manage DRM as an external third party provided service, some level of DRM functionality may need to be provided within the community, to the extent that enforcement is possible.

The DRM component acts as an interface that allows content owners, community members and community operators to set additional policies using the *Policy Management* component that are community-specific (e.g. defining community-wide licenses, community-wide usage conditions, etc).

For example, if a content owner provides a usage license for a community, some interaction is required between the DRM system (which enforces the rights) and the community platform to share information on who is currently a member of that community.

DRM may also be provided at the client.

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

E.46.3 Dependencies

Components that this component calls	Purpose
Access Control	To control access to content.

Components that call this component	Purpose
Consent Management	To enforce member-specific DRM.
Policy Management	To enforce community-wide DRM.

E.46.4 Drawing

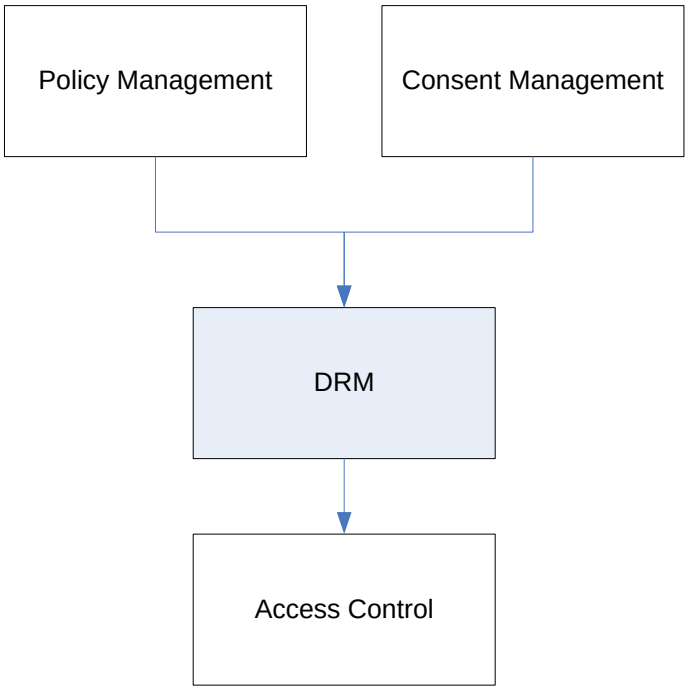


Figure 113 DRM

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

E.47 Linkability

T_2 $PICOS_{distinguishing}$ $PICOS_{research}$

PICOS Principle (PP): 2, 3, 8, 11, 18

PICOS Feature (PF): 1, 2, 10, 15

E.47.1 Purpose

The *Linkability* component determines if a link can be established between independent events.

E.47.2 Description

Linkability is the ability to link together pseudonyms, posts or other events performed by a single entity (member). The main contribution of the *Linkability* component is a profile of activities performed by a single entity. The more sources of information available, the more information can be linked together and this has a direct impact on the quality of the profile. Well created member profile may contain very sensitive information.

Providing anonymity and unlinkability increases member privacy. However, identification and linkability provides easier accountability/non-repudiation and tracking. Between the two extremes of complete unlinkability and easily visible linkability there is a range of options where events can be only linked with additional knowledge or with the parties collaboration of one (though typically several) trusted party.

The Linkability component provides two roles:

- Resolving linkability: When required, this component will assemble the necessary information to prove a link between a member and contributed content, or identify a member from contributed content
- Providing unlinkability: Several techniques exist that provide unlinkability, but they are generally designed for specific situations, e.g. message transfer, group signing (where the actual signer does not want to be identified other than a member of the group. For each situation, a range of actions will need to take place, and the role or the Linkability component is to co-ordinate the various components and service that will provide the solution, e.g. key management, cryptography, authorisation.

At present the *Linkability* component will access the *Privacy Adviser* component in determining where excessive linking is taking place. It is possible that the *Linkability* component can assist legislation, non-repudiation, anonymity and accountability.

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

E.47.3 Dependencies

Components that this component calls	Purpose
None defined at present	To control access to content.

Components that call this component	Purpose
Privacy Advisor	To determine the extent of linkability.

E.47.4 Drawing

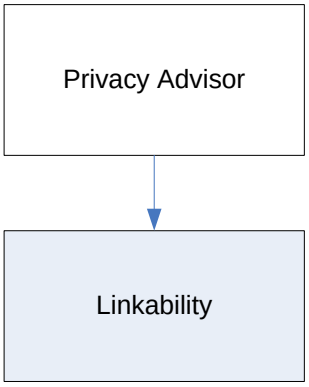


Figure 114 Linkability

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

E.48 Non-repudiation

T_2 PICOS$_{enhancing}$

PICOS Principle (PP): 1, 12, 14, 23

PICOS Feature (PF): 15

E.48.1 Purpose

The *Non-repudiation* component provides a non-reputable binding.

E.48.2 Description

In order to provide a suitable support for accountability within PICOS, all members' contributions should provide a (direct or indirect) non-reputable binding with the originating member.

This *Non-repudiation* component adds a non-reputable binding to all content that is contributed to the community. Alternatively, it can provide optional ‘on demand’ binding or component and originator ID to yield the corresponding non-reputable binding.

A further option is for the contribution to be digitally signed at the client using the private key of the contributing member, possibly the same key that the member uses when authenticating themselves to the community. In this way the community can verify the authenticity of the contributing member and the content before acceptance.

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

E.48.3 Dependencies

Components that this component calls	Purpose
Cryptography Key Management	To provide cryptographic primitives, e.g. digital signature.

Components that call this component	Purpose
Content Sharing	To provide provenance of contributed content.
Event Logging	To maintain integrity of event information.

E.48.4 Drawing

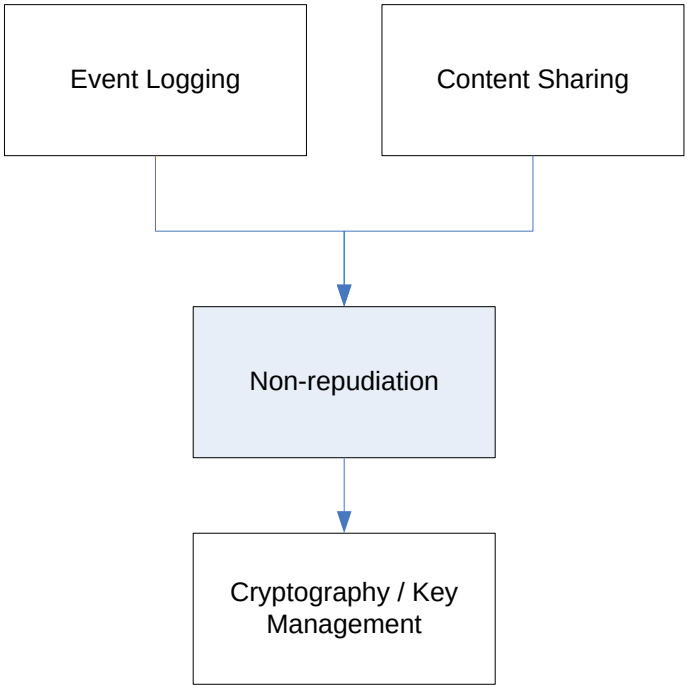


Figure 115 Non-repudiation

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

E.49 Secure repository

PICOS D4.2 new/updated component

T2 PICOS enhancing

PICOS Principle (PP): 4, 10

PICOS Feature (PF): 2

E.49.1 Purpose

The *Secure Repository* component provides a safe location to store personal sensitive information.

E.49.2 Description

The *Secure Repository* component provides a safe place to store content and security-related data (e.g. keys) on the client or in the community. Content can be text, audio or video contribution by a member.

All member data needs to be stored in a secure location, i.e. encrypted on the client or community. The reason for this is to protect member data in case the client device is lost or stolen, and to prevent others gaining unauthorised access to private sensitive data.

The *Secure Repository* component interacts with the storage medium to store and retrieve content. In one mode, the Encryption/decryption takes place within the component so that content transferred to the medium is protected. Therefore the component will need to be provided with appropriate keys.

Alternatively, content can be provided to the component in encrypted form.

Where the component provides the encryption, it will only do so after receiving a valid authentication from the content owner. Authentication is achieved with support from the *Access Control* component and *Authorisation* component.

The new fields supported in Gamers community are:

- Street Name
- Locality
- Facebook
- Phone Number
- Internet Access
- Favourite games
- Favourite location
- Alliance memberships

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

- Playing style
- Travian epochs
- Blank field

E.49.3 Dependencies

Components that this component calls	Purpose
Cryptography Key Management	To provide cryptographic primitives, e.g. digital signature.

Components that call this component	Purpose
Access Control	To retrieve identity information.
Authorisation	To retrieve authentication information.
Cryptography Key Management	To provide cryptographic primitives, e.g. digital signature.

E.49.4 Drawing

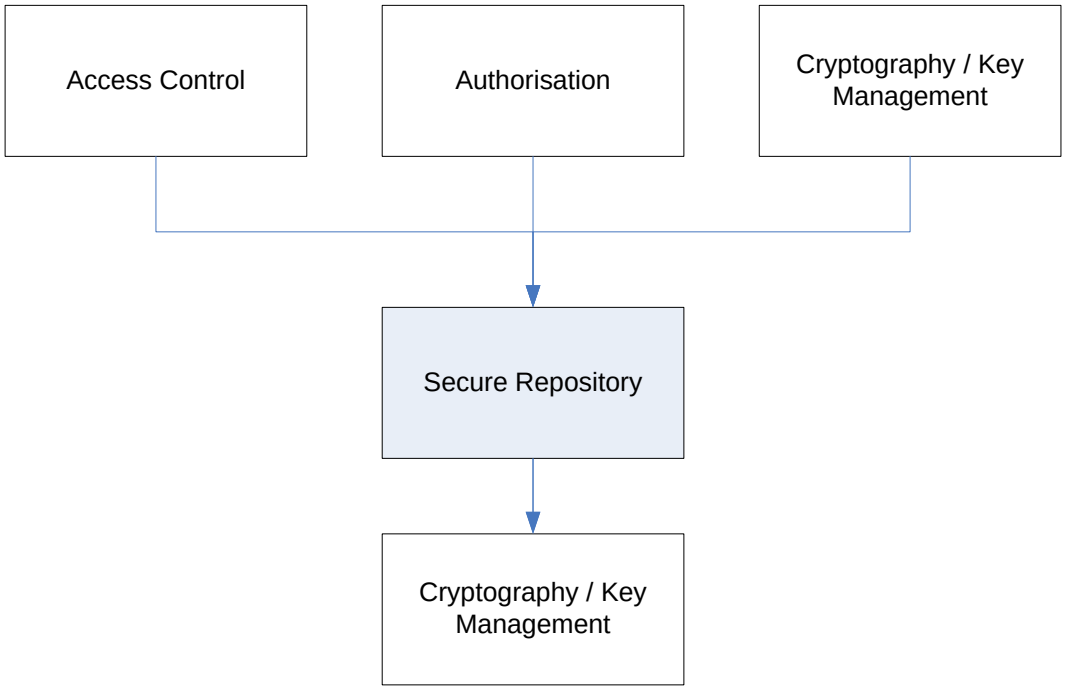


Figure 116 Secure Repository

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

E.50 Contacts management

PICOS D4.2 new/updated component

T2 PICOS enhancing

PICOS Principle (PP): 1, 2, 3, 4

PICOS Feature (PF): 3, 7, 10, 12

E.50.1 Purpose

This new functionality added for Gamer Community displays the contacts list for a selected contact from the user's contact list, where the selected contact has created a privacy rule allowing this task, i.e. "I allow my contact list to be seen".

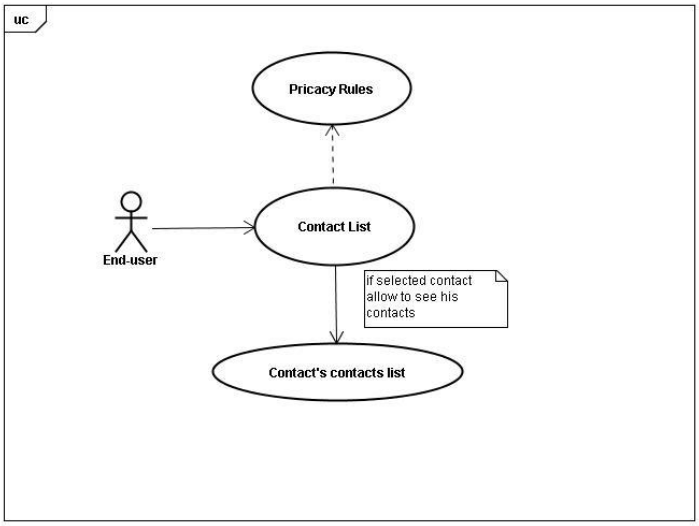


Figure 117 Contacts Management

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

E.51 Public Community

PICOS D4.2 new/updated component

T2 PICOS enhancing

PICOS Principle (PP): 6, 9, 13, 22, 23

PICOS Feature (PF): 1, 2, 9, 13

E.51.1 Purpose

The public community use case is extended to support the following features:

Attach Privacy Rules to Content

Applied when Forum Threads are public Repository (repository Categories and categories Files). This means that only Contacts selected by user will have access to the Thread Posts, or Categories Files for a valid period of time.

Subscribe/Unsubscribe to new Available Content

User will receive a notification from the Platform when a new content is available into the selected forum Thread or repository Category.

Retrieve the Content Access History

Allow retrieving the access history (this is the person pseudonym that accessed to the content and the access date) for a selected POST within a forum Thread, or selected File within a repository category.

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

E.51.2 Description

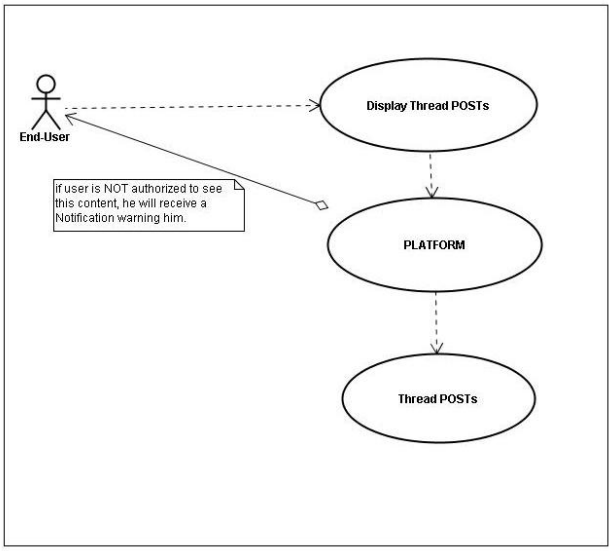


Figure 118 Thread Privacy Rules

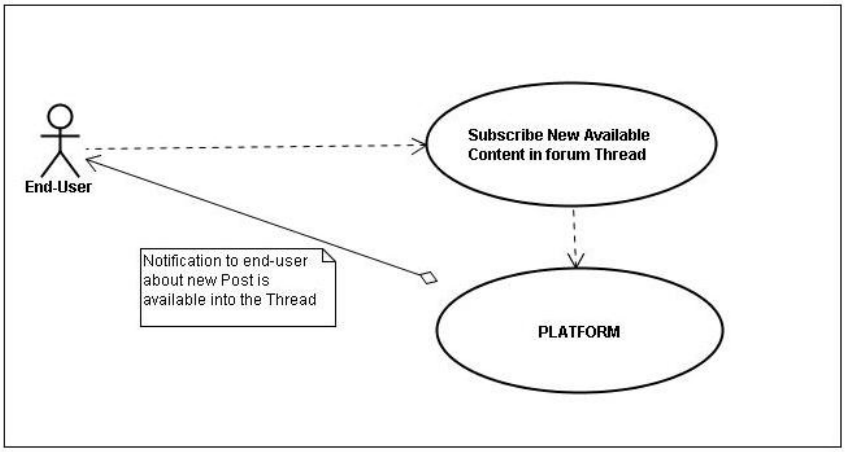


Figure 119 Subscribe new available content

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

E.52 Share Desk

PICOS D4.2 new/updated component

T_2 PICOS enhancing

PICOS Principle (PP): 11, 13

PICOS Feature (PF): 2, 7

E.52.1 Purpose

The idea is offer a place created by one user where he can publish content. The user selects among his contacts a list of community members that can access (read only) the shared desk.

The proposal is to use the basic mechanisms of a private sub-community where users are invited. The major difference is that this "shared desk" sub-community allows the creator to write and read content whereas the invited users can only read content. The second difference is that the shared desk invitations are time bounded. The third difference is that the shared desk does not offer forum facilities.

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

E.53 Location Base Services

PICOS D4.2 new/updated component

T2 PICOS enhancing

PICOS Principle (PP): 4, 11

PICOS Feature (PF): 8

E.53.1 Purpose

This second PICOS prototype offer new location based services which were not available in the first one. The next points will describe these new services: Private Sites, Points of Interest (POI) and meeting with nearby players.

E.53.2 Description

Private Sites

This is a new concept introduced in Picos project and it refer to an private area (GPS coordinates + radius parameter, title and site description) where the end-user is able to attach privacy rules in order to state who (what Contacts) will be authorized to see his location information when he is close that private site.

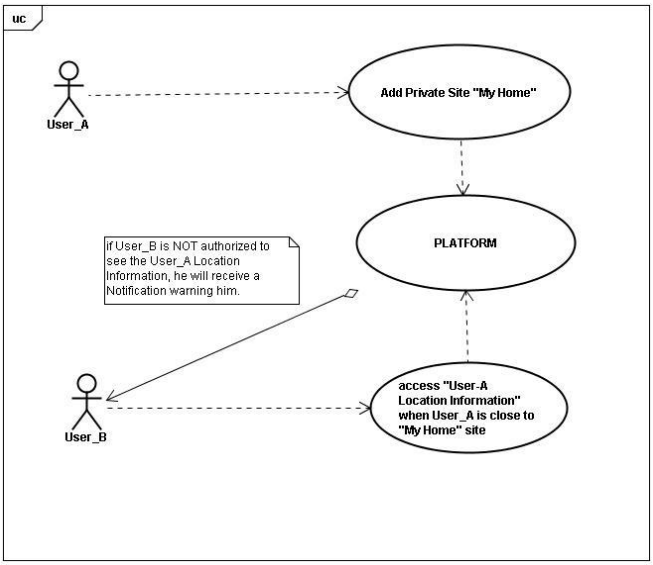


Figure 120 Privates Sites

Points of Interest (POIs)

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

This is another location based service provided in the Gamers prototype which was not supported in Anglers prototype.

Points of Interest are defined as a location with attributes including GPS coordinates, a description and the POI type (for instance internet cafe, game shop, etc.).

The POIs will either be private or public and there will be a set of pre-defined POI types. It will be also provided a POIs searching mechanism.

The user will be able to perform the following associated tasks:

- Add a new POI
- Delete a selected one
- Edit a selected one
- Rate/Comment the POI
- Reload (list) all POI
- Show POI details
- Show POI on map

Besides these possibilities it will be added as well the option of marking a place on a map as a Point of Interest

Meeting with nearby players

The goal of this service is to offer search facilities to detect PICOS users in an area (centre and rectangle dimensions). Once the list of user is sent back, the user has the possibility to launch a real time chat or send asynchronous messages with the list of a sub list of the nearby users. Once the chat is closed, the user can decide to add these users as contacts.

The list will be composed of users that are making their location information available. If they have restricted access in place on their location information (privacy rules) , they will not be part of the returned list.

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

E.53.3 Drawing

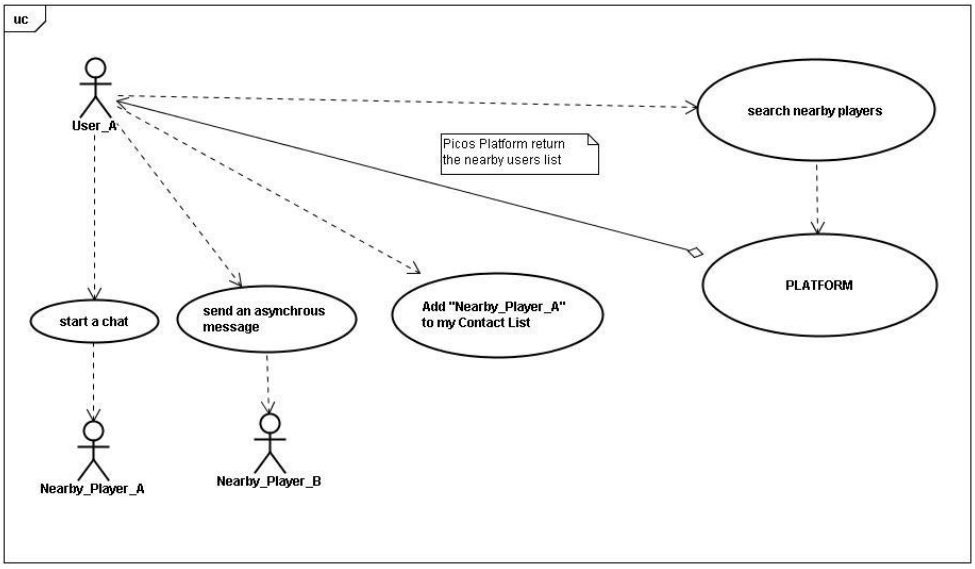


Figure 121 Meeting with nearby players

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

E.54 Advertising Services

PICOS D4.2 new/updated component

T_2 PICOS enhancing

PICOS Principle (PP): 3, 4, 13

PICOS Feature (PF): 9, 13

E.54.1 Purpose

Gamer Community will support Advertising Services, which allows advertisers to configure advertisements. Thereby PICOS Community acts as an intermediary, who mediates between Community user and advertiser and delivers the advertisements on behalf of the advertiser and based on users personal data. The personal data of the users remains within the community and is not directly accessed by the advertiser.

E.54.2 Description

The Advertising service implementation on client application will based on POI implementation, therefore when user (advertiser) wants to create an announcement he must go to "Add POI" screen and enter the advertisement data: title, description, key words, location data, type, and target users for receiving that announcement. The advertiser can select among the following target users type:

- Age (from X to Y, e.g. "from 20 to 40")
- Gender (Drop-Down-List: male only, female only, male and female)
- City (Drop-Down-List: Brno, Vienna, Madrid, Frankfurt)
- Interests (Check Boxes: Games, Music, Friends, Bars, Internet Cafés)
- Favourite Games (Check Boxes: Travian, Counterstrike, World of Warcraft).

So only these target users will receive the announcement, if they would have subscribed previously to receive announcement.

Other functionality supported by Gamers Community related to Advertising is to recommend an announcement, this is, when one target user receives an announcement he might recommend it to his Contacts if he consider it interesting, and therefore his contacts will receive the announcement in case they would have subscribe previously to receive Recommendations.

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

E.54.3 Drawing

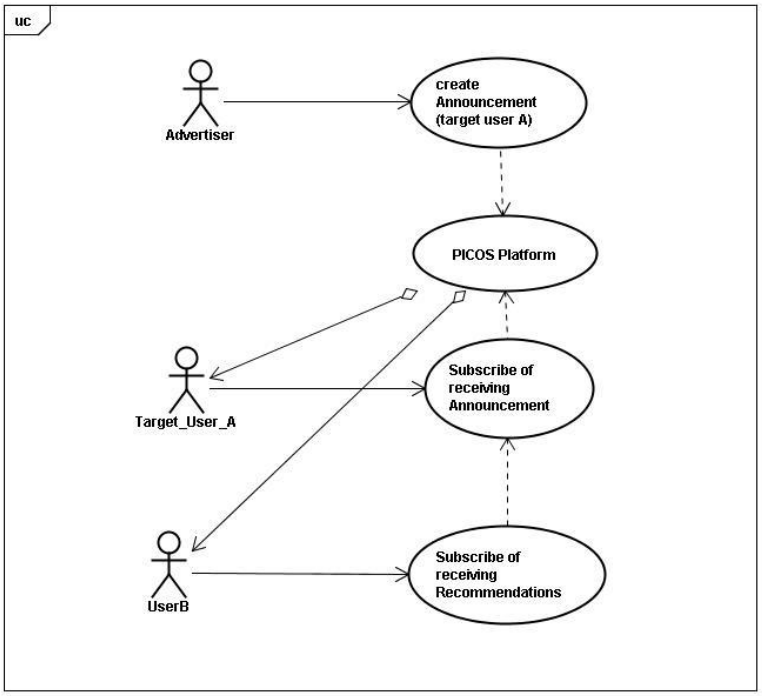


Figure 122 Advertising services

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

E.55 Alarms

PICOS D4.2 new/updated component

T_2 PICOS enhancing

PICOS Principle (PP): 4, 14

PICOS Feature (PF): 12

E.55.1 Purpose

This would be a desirable functionality for Gamers Community, this would be to give user the chance of defining a set of alarms which leads to notifications to the requester as well as set of predefined destination (among his contact).

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

E.56 User Availability Calendar

PICOS D4.2 new/updated component

T2 PICOS enhancing

PICOS Principle (PP): 3, 4, 10

PICOS Feature (PF): 8, 10, 12

E.56.1 Purpose

The same than alarms case this functionality would be desirable as well. This means to give user the option of setting an availability calendar and to share this calendar with his contacts.

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

E.57 Archive Chat

PICOS D4.2 new/updated component

T2 PICOS enhancing

PICOS Principle (PP): 3, 4, 23

PICOS Feature (PF): 5, 11

E.57.1 Purpose

This would be another desirable additional functionality for Gamers prototype. It implies to improve the chat component from Anglers prototype.

The real time content sharing component of Anglers prototype already stores all chat message exchanges and archive it but doesn't provide an interface to retrieve them. Then the improvement for Gamers would be to offer an interface to retrieve the list of chat, the user has been part of, and for which the chairman has decided to archive.

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

Appendix F Summary of Angler and Gamer requirements for second prototypes

F.1 Necessary

- REQ : Gamers R1: Sharing Contact-List
- REQ : Gamers R3: restrict access to published content
- REQ : Gamers R4: restrict access based on date condition
- REQ : Anglers R34: Enhance Content Awareness
- REQ : Anglers R36: social presence awareness (POI)

F.2 Recommended

- REQ: Gamers R5: Notification for new available content
- REQ: Gamers R7: Content access history (public community)
- REQ: Gamers R16: public Point of interest
- REQ: Gamers R19: custom POI
- REQ: Gamers R20: private or public POI
- REQ: Gamers R23: Advertising services
- REQ: Anglers R37: revocation

F.3 Helpful

- REQ: Gamers R9: Shared desk (combined with +R12)
- REQ: Gamers R10: Real chat
- REQ: Gamers R13: Reminder (notifications)
- REQ: Gamers R14: Reminder (sharing)
- REQ: Gamers R15: enriched status information
- REQ: Gamers R17: meeting with nearby players
- REQ: Gamers R21: Real time content sharing
- REQ: Gamers R22: archive chat
- REQ: Anglers R26: Offline notifications

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

Appendix G Result of Gamer questionnaire

G.1 Questionnaire

The questionnaire was originally published in Czech language so there can be a slightly different understanding of the meaning between the original Czech version and its translation into English.

1. How important is communication, collaboration and interaction with other players in Travian?
2. How do you make the first contact with other players and how do you manage contacts you already have?
3. How is your community (your alliance or a group of cooperating alliances) organized? How do you manage contacts on players from cooperating alliances?
4. Are you in contact with other players (online, real meetings) beyond the game? If so, what kind of communication tool you use (social networks, ICQ, Skype, email, personal meetings)?
5. Do you play with mobile devices?
6. If so, what devices you use (portable laptop, PDA, mobile phone ...)?
7. If not, why? Can you image to play the game with/on a mobile device?
8. How much time (on average) do you spend with playing?
9. What kind of information do you share (or would like to share) and with who (within the game)?
10. What are the most critical aspects to get and loose reputation (or respect of other players) during the game?
11. Is your differentiation of who do you trust on a group-based or individual-player-based level?
12. Are you a member of any other online communities (other online games, social networks – Facebook, MySpace ...)?
13. Are there any players you stay in contact beyond the game (going to pub sometimes, sharing the university dorms ...)?
14. Do you share some private information that are not necessary for the game (postal address, phone number, email address ...)?
15. What would make you change you alliance in the game? What were your reasons for changing the alliance in the past?
16. Do you buy Travian gold coins? Would you be willing to pay for the possibility to play the game? What amounts?
17. Will you accept advertisements in the game if these will be adjusted to your needs (long term preferences, restaurant nearby your geological location ...)?
18. What benefits would you expect in exchange for the advertisements?

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

19. Can you imagine being a member of a wider (Meta) community (and the respective system), that would manage your contact from all games you are playing?
20. Which additional services (beyond the standard Travian services) would you be interested in (better discussion board, possibility to communicate securely within an alliance ...)? What are the issues related to the Travian game, that you manage outside the official Travian game environment?
21. Are you willing to put together contacts you get during playing with your personal/private contacts (family, friends, workmates ...)?
22. To what extend do you trust Travian developers in managing your in-game information (so that, e.g., do not forward this information to another alliance(s))?
23. To what extend do you trust Travian developers in managing personal information (real name, postal address, email address, phone number ...), that you provided during registration?
24. What makes Travian interesting for you when compared with other online games? What are the interesting features/functions?
25. What kind of personal information did you provide in the Travian game (your real name, age, education ...)?
26. Would you benefit from technological support of individual players reputation? Reputation is meant as a set of indicators how a player behaved in the past, how did he/she reacted on a given task or how often did the player changed the alliance?
27. Are there any non-written rules defined in the game? Something that is not controlled by the Travian server but majority of players follows such rules. What are the rules for players in your alliance?
28. What happens if a player does not follow the general rules in the alliance? Is there any global evidence and investigation of sinners (by e.g. the leaders of the alliance)?
29. What do you imagine under the term “privacy”?
30. Is anonymity/pseudonymity in or outside the game an important feature for you? Anonymity – nobody can see your real identity. Pseudonymity – you are known under your nick but there is no link to your real identity.
31. Are there any privacy supporting tools/services available in the Travian game? Are there anything you miss in the game and it would be good if this would be available?
32. What are your expectations about the functionality of mobile infrastructure for playing the game (e.g. checking your villages, sending support, contact other players)?
33. What would be the benefits of being able to play the game with a mobile device (in a situation that other players don’t have such option)?
34. What would be the preferred game functionalities you would like to have with/on a mobile device (e.g. check the status of your villages only) and with your home PC (e.g. sending attacks)?

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

G.2 Summary of results

The questionnaire from the previous sub-section was given (in Czech language) to a members of one strong alliance during the last third of a game epoch. The following list provides the global summary that was at a start of the gamers' prototype the main source of feedback to formulate the gamers' requirements.

1. Communication and information sharing are the most important aspects of the online game. Players communicate very often, those who now each other quite well are also seeing each other in real. Players are typically open to mix-up their personal contacts (family, friends, and workmates) with contacts they got from the game.
2. Gamers typically use build-in systems to keep their contacts. Once the game is over, this contact list is unavailable. Some players keep the most important contact e.g. in their Skype/ICQ accounts or even in their mobile phones.
3. Organization within the alliance varies from alliance to alliance. Better organization typically means stronger alliance. Players responded that the organization of alliance is typically ad-hoc without any kind of stable structuring.
4. Players use typically their home PC or notebooks for playing. Some of them responded that if it is necessary they also use their mobile devices but the comfort of playing is very low. Those who never used a mobile phone for playing can imagine such possibility but only in extreme situations. They won't play the game on a mobile device if there is a possibility to use laptop or PC.
5. On average (if we can make such estimation), players spend 20+ hours of playing every week. At the final stage of the game epoch, this number can increase significantly.
6. Information that is shared among members of an alliance is variable but the required minimum is the number of troops, their location and power and amount of resources (food, wood, building material). Some players would appreciate the possibility of selective distinction what they want to share and with who (with even the "when" option).
7. Trust is a very sensitive indicator in the game. Trusted players are very valuable for the alliance. It is also good if a player would have a possibility to prove/show his past activities in the game in order to convince the alliance leaders that he/she is reliable player. Players are typically assessed as individuals (in terms of trust). Membership of a trustworthy alliance does not mean that all its members are necessarily trustworthy. Players in general do not trust game developers very much. The reason is that developers are part of the game (they have to look after the server where the epoch is played) and therefore they could get more information than ordinary players. Players do not see a big risk regarding the data they provided during the registration. Simply because they can insert fake data.
8. When the answers were collected nobody was a member of any social network. But this would have probably changed.
9. Personal information that is typically shared is postal address, email address and phone number. Phone number is good in case of the need of urgent communication.
10. Players would change their alliance in case that the alliance doesn't work as a whole, has non-trusted players or their friends also changed the alliance.

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

11. Players buy Travian gold coins quite often. It improves the functions they can use while playing. Some people also use special tools (simulators, troop's strength calculators, time and distance calculator). Some of these tools are freely available, some of them are paid.
12. Regarding the advertisements, the responses were half/half. Targeted advertisement can sometimes be useful but its better to have a game free of ads. If there is an advertisement, players would accept it in exchange for, e.g. the gold coins.
13. Players do not see (at the time of providing their answers) too much benefit from being a member of a wider community then their alliance. Some of them replied that they simply do not want to be a member of such social network while others felt some possible privacy sensitive issues (e.g. user profiling).
14. The most required thing besides the one provided in the game was the discussion board. With an external discussion board, players can do whatever they want without (possibly) being observed by the game developers. The other required functionality was good statistical information about individual players and their past activities within the game and support for cross-alliance communication and contracts agreements.
15. Players like the Travian game because it's a good game (some of them provided us with some basic comparison with other online games), it has quite simple rules and the players meet other people who they cooperate with.
16. Players would really appreciate having some technological system in order to see other player's reputation score. This would help to distinct between good and bad players (from the long term prospective).
17. Players feel the term "privacy" as information about their lives, work, and family. Private information is sensitive and they would like to control who has access to this information and for which purposes.
18. Anonymity as a feature is not considered as necessary in the game because everybody is using a nick-name. This is a form of pseudonymity but there is no linkage to the real indemnity (at least in the case that the player keeps changing his nick and do not use one nick for a long time). Some identity management system would be useful.
19. The only privacy-related information in the Travian is the online/offline status which can be indirectly observed by sending a message to a player whose status is to be observed. Within the alliance, there is a status bar of all its members so that others can see whether they are online or not (or even when they were online for the last time).
20. If the game is to be played with/on the mobile phone, the comfort of playing must be comparable with laptop or PC. But many players responded that they prefer computers and mobile phones are used only in critical situations. The use of mobile phones also helps to be online almost all day. Required feature would be some kind of notification of an incoming attack via SMS.

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

Appendix H Link from Requirements to Component

The Table below shows for all components where the corresponding requirement arose and how the connection to PICOS Principles and PICOS Features was established.

In the following table, the code used to reference requirements is:

- Rx R1/R2 Investigation requirements
- Rx.xx D2.4 requirement
- PICOS Requirement originating from PICOS team

H.1 Tier 1 Components

Requirement	PICOS Principle	PICOS Feature	Component Name
R3, R4, R2.12	3, 17	3	Access Control
PICOS	13	9, 13	Application Orchestrator
R1.13, R1.14, R4.11	1, 14	1, 15	Audit
PICOS	1, 4, 7, 10, 20	11	Communication Management
R3.4, R3.6	11, 17, 18	1, 3, 4	Identity Lifecycle Management
R3.12	2, 3, 4	2, 5, 6, 10,12	Importer/Exporter
R1.13	4	13	Intrusion Detection
R5.5	5, 10	14	Preparation Area
PICOS	19	7, 10	Sub-community Management

Table 11 Link from Requirements to Components – Tier 1

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

H.2 Tier 2 Components

Requirement	PICOS Principle	PICOS Feature	Component Name
R3.1	1, 17	3, 15	Accountability
R23, R3.5	3, 4, 13	9, 13	Advertising Services
R1.13	4, 14	12	Alarms
R3.4, R3.9, R3.14, R3.19	1, 4, 8, 11	2, 5, 9, 13	Anonymisation
R10, R22	3, 4, 23	5, 11	Archive Chat
R3, R4, R2.12, R4.5	3, 17	3	Authentication
R4.5	17, 18	3	Authentication Method Selection
R4.5	3, 17	3	Authorisation
R2.12, R3.5	2, 3, 4	2, 10	Consent Management
R1	1, 2, 3, 4	3, 7, 10, 12	Contacts Management
R5, R7, R14, R21, R34, R36, R2.11, R5.10	4	2	Content Sharing
R2.3, R2.5	1, 4, 8, 9, 17	1, 3, 10, 15	Cryptography / Key Management
R37, R2.1	3, 8	2	Data Minimisation
PICOS	12, 23	1, 2, 10, 15	Date/Time Stamper
R37	2, 23	3, 7, 15	Delegation
R37	2, 10, 23	2	DRM
R3.15	1, 5, 14, 20	1, 15	Event Logging
R3.14	1, 20, 23	1	Event Reconstruction
R3.12, R3.123	6, 16, 22, 23	1	External Recommendation
R3.12, R2.4, R4.8, R5.7	6, 13, 17, 22	10	External Service Delivery
R1.14	5, 16, 23	1	Feedback Management
R2.10, R3.4	6, 13, 18	9, 13	Identity Translator
R3.4	2, 3, 8, 11, 18	1, 2, 10, 15	Linkability
R15, R16, R17, R19, R20, R36, R5.12	4, 11	8	Location Based Services
R5.12	10	4, 8	Location Sensor

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

Requirement	PICOS Principle	PICOS Feature	Component Name
R4.10	1, 4, 7, 9, 10, 11, 13, 20	11	Network Security
R3.2, R3.10, R4.1	1, 12, 14, 23	15	Non-repudiation
R37	10, 13	5, 11, 12	Notification
R13, R14, R5.4	1, 4, 7, 9, 10, 11, 13, 20	11	P2P Communication
R2.10, R3.4	11, 18	1, 3	Partial Identity Management
PICOS	3, 4, 9, 13	9	Payment Services
R2.7, R2.9, R4.4	1, 3, 5	2, 3, 11, 13	Policy Management
R26	3, 4, 8	2, 10	Privacy Advisor
R4,4	3	2, 3	Privilege Management
R2.7, R2.9, R4.4	4, 23	4, 8	Profile Management
PICOS	6, 9, 13, 22, 23	1, 2, 9, 13	Public Community
R1.12, PICOS	21, 23	1	Recruitment
R3.14, R3.17, R4.1, PICOS	17	3	Registration
R1.11, R3.2, R3.7, R5.11	6, 22, 23	1	Reputation Management
R37, R3.7	2, 12, 23	2, 10, 15	Revocation
R3.6	8, 11, 23	2	Scenario Management
R3.11	4, 10	2	Secure Repository
PICOS	11, 13, 17	9, 13	Service Selection
R9, R2.11	11, 13	2, 7	Share Desk
R5.12	10	8	Social Presence
R1.1, R1.2, R1.3, R1.4, R1.5, R1.8, R1.9, R1.11	6, 16, 22, 23	1, 15	Trust Negotiation
R3.19	1, 2, 6, 12, 22	1, 3, 9, 13, 15	TTP Management
PICOS	3, 4, 10	8, 10,12	User Availability Calendar

Table 12 Link from Requirements to Components – Tier 2

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