W3C - Workshop on the Future of Social Networking – Position Paper

Alberto Crespo, Rubén Méndez (ATOS ORIGIN) and Katja Liesebach (Goethe-Universität Frankfurt)

PICOS – Privacy and Identity Management for Community Services

Climbing towards trust and privacy management in social mobile communities

Background

In recent years, we are witnessing the emergence of services which, coupled with new technologies, act as enablers for professional and private on-line collaboration via the Internet. This is creating new opportunities and challenges worldwide, both for individuals and for the ICT industry as a whole, leading the evolution of the Internet toward a more pervasive and user-centered based model where ambient intelligence and smart devices play an increasingly preeminent role. Nowadays, many European citizens spend work and leisure time in on-line communities, such as social networks or other real world communities that make use of on-line services to support their activities. The convergence of powerful communication and computing capabilities in smart devices, coupled with their intrinsic ubiquitous nature, enable community members and other involved stakeholders, to participate at the place and moment of their choice and in the way they prefer.

Mobile communities also allow for a more intensive linking of services and consequently for the integration of people's virtual and real communities, supporting individuals in performing professional and leisure tasks through enhanced collaboration workflows and allowing to access informational assets of great added contextual value. In this respect, context-related information and services, such as location-based services, are rapidly taking off in their availability and consumption by community members, e.g., for spontaneous socializing and collaboration in the "real" world. However, when users participate in such communities, they unconsciously leave private information traces they are unaware of and, even when they provide on purpose personally identifiable information, they are usually not aware of their rights and of undesirable consequences in case of misuse.

The providers of community services need to handle trust and privacy in a balanced manner that meets the participants' needs and complies with existing regulation. Moreover, the business models of communities offering such services (i.e., social networking sites) often lead to the need of opening their infrastructures to other stakeholders (like third-party service providers) and to accommodate marketing activities of sponsors/advertisers. As new community-supporting services offered by communication service providers need to become increasingly interoperable, provisions that have to be put in place for trust enablement and privacy-respecting identity management will also require procedural and technical mechanisms to increase their own interoperability.

A new approach to identity management in community services is needed, in order to meet needs with relation to:

- The enablement, by members of the community, of trust in other members, community-related stakeholders and in the service-provision infrastructure itself,
- the privacy of community members' personal information,
- the control by members of the information they share, and
- the interoperability of community-supporting services between communication service providers.

This approach must be developed in an open manner, and requires technical and procedural advancement in order to meet the requirements.

PICOS project

The project name, PICOS, is an abbreviation of “Privacy and Identity Management for Community Services”. The main goal of the project, funded in the frame of the 7th European Framework Program, 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. This will be done in parallel to the research needed to address the most serious security challenges faced by the public and private sectors and especially by European citizens who have the right to benefit from safer on-line mobile communities.

PICOS partners understand the deep necessity (through a methodical approach to assessing the various threats and risks related to mobile and on-line communities, trust and privacy) for multidisciplinary research on the facets of community-based on-line interaction: for instance, technology developers need a much deeper understanding of the social, legislative needs and limitations than they can discover through the exclusive study of technology itself. Newly-developed on-line communities will benefit not only from PICOS philosophy and best practices driving innovative engineering and design principles which can be built into architectures and frameworks from their inception, but also from a rich set of tools, components, services and technologies that can be easily adopted too by existing on-line communities. In particular, PICOS will examine the role of Privacy-Enhancing Technologies (PETs), portable reputation systems and user-centered identity management schemes (together with portable reputation systems and user-centered identity management schemes), with the aim of empowering mobile community stakeholders to choose the most appropriate tools and frameworks to satisfy and reconcile their respective needs and interests.

The PICOS project will address the following main questions:

- What are the Trust, Privacy and Identity issues in new context-rich mobile communication services, especially community supporting services?
- How can information flow needs and privacy requirements be balanced in those services, especially in complex distributed service architectures (e.g., mash-ups)?
- How can all of these issues be solved in an acceptable, trustworthy, open, scalable, manner?
- Which supporting services and infrastructures do the stakeholders (e.g., communication service providers, community service component providers and aggregators, community administrators, professional and private users, advertisers/sponsors, etc.) need?

For answering these questions, the PICOS approach is to research, develop, build, trial and evaluate in an open and integrative manner a privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile communication service providers. It emphasizes further the applicability of the platform to community business models. In two development cycles the PICOS platform will be consolidated. The purpose of the first cycle is to create and validate the platform architecture and design concepts and their acceptability from a user experience viewpoint. In contrast, the second cycle is to provide a richer, more balanced and capable platform, with an end-to-end scope.

In its first cycle, PICOS will investigate, characterize and categorize various types of communities and their stakeholders in order to develop a multidisciplinary set of requirements with particular focus on trust, privacy and personal information for the platform. Based on that requirement set, PICOS will develop an architecture and a design for this, and validate them by constructing community service prototypes. These will be trialed and the results analyzed. The results of all the above will be evaluated by the project and used to specify revised requirements for the platform. Following, a second cycle of platform architecting, platform design, service prototype construction and trialing will be performed, and the results will be accordingly evaluated. Evaluations will be undertaken with the participation of a well-defined set of members of exemplary communities, where this is appropriate. Additionally, the project will include technical and overall quality assurance activities and, moreover, it will also include activities to disseminate the results. The PICOS project will allow insight from broader interrelated areas to guide the strategic focusing of the European research agenda. PICOS holds multiple liaisons with key Framework Programme 7 Projects, such as PRIMELife[1], My-eDirector 2012[2] and Turbine[3], the FP 6 project FIDIS[4], and international standardization bodies like ISO/IEC SC 27 WG 5.

Through the diversity of the PICOS consortium which brings together representatives of academia, vendors and system integrators, telecommunications and user communities of seven European countries, the necessary sets of expertise and validation abilities is given to cooperate and work towards the project objectives.

At this stage, PICOS concludes its first phase which is aimed to provide the basis for the design and development of the PICOS platform while taking advantage of the multidisciplinary of the PICOS consortium. Based on an initial description of the underlying terminology which attempts to consolidate the perspectives of different research disciplines, special focus was put on a classification approach for communities. As diverse the intentions, organization and used technological framework of communities are, as challenging is the compilation of a catalogue which reflects the needs and requirements of the involved stakeholders. Nine major dimensions depicting PICOS' problem space have been identified allowing more flexibility in dealing with new and/or emerging communities in the era of Next Generation Networks. This categorization approach was fortified by a comprehensive and quantitative questionnaire (feedback has been provided by 856 participants) addressing user's privacy preferences, requirements and usage of privacy settings in different usage contexts. The questionnaire substantiated significant differences in the behavior and needs of users with regard to the type of community, especially between sites intended for social networking (private vs. business) and sites where networking and the provision of data serves are secondary. Besides the categorization activity, the second main pillar towards the PICOS platform to be developed is formed by the contextual framework in which disciplines, influences and context of that platform are gathered in order to deliver influential trends and to provide a meaningful context for research and application of the PICOS innovations. On top of these pillars, community-specific and -general requirements have been identified while involving stakeholders of exemplary communities (covering the range of private and professional communities) into this process. The complex feedback given by community stakeholders has been categorised, explained and backed by rationales why the stakeholders have vital interest that the stated requirement becomes addressed. It has finally led to a list of challenges which have to be weighted and transferred into technological and organisational measurements to support today's and future mobile communities.

ATOS ORIGIN's Role within PICOS

ATOS ORIGIN supports PICOS holistic approach to the central issues at stake, involving cross-disciplinary legal, social, cultural, organizational and economic/business aspects, trying to provide a thorough and sound understanding of the complex interrelationships and dependencies involved and developing the appropriate technical expertise and solutions to support the communities' needs for privacy, trust and identity management. More specifically, ATOS ORIGIN leads the implementation effort for the PICOS Community Application Prototypes which will serve to operationally validate PICOS technologies and vision for selected scenarios belonging to a real on-line community. Provision of adequate procedural and organizational measures is critical for the security aspects involved, and these are also points of interest for PICOS, taking into account the range of potential organizations which may benefit from advances in

[1] http://www.primelife.eu/

[2] http://www.myedirector2012.eu/

[3] http://www.turbine-project.eu/

[4] http://www.fidis.net/

the context of the project. Integration with standard legacy IT infrastructure of existing communities and upgrading existing on-line networks to leverage them with PICOS specific technologies and approaches is another fundamental focus of interest for ATOS ORIGIN as is the understanding of the structuring of social networks and how complex relationship dynamics influence not only different requirements and usage habits but also the possible business models and opportunities for the different stakeholders involved. Thus, for example, mobile communication platforms developed taking into account PICOS results would greatly benefit both the mobile service providers industry and the mobile consumers who would enjoy enhanced overall security and would be thus more confident to trust reliable mobile infrastructures and services).

We are convinced of PICOS' role in helping both industry and research communities by analyzing and balancing different stakeholders interests (i.e., advertisers or service and third-party providers versus community members). PICOS can also analyze tradeoffs for seemingly irreconcilable dichotomies between privacy and other important societal values (i.e., privacy vs. convenience/profitability /accountability/ efficiency etc.) towards leveraging community win-win scenarios which could simultaneously protect privacy, foster trust, securely manage identities and satisfy alleged antithetical interests.

We believe in PICOS that promoting a proper adoption of standards and the conformance to established assurance and certification criteria is advisable in IT projects intended to support or build secure social networks and other types of on-line communities, in combination with well-focused, objective-aligned and consistent architectural, design and development activities reliant upon industry-respected best practices. We assume that one of the most relevant fields for research in the privacy area in the following years will be that of methodological approaches for systematic analysis, prediction and assessment of risks related to privacy and identity management, given the fact that the role of risk analysis has become a key activity in the challenge of building trust for citizens and consumers in the virtual world and correctly planning strategic positioning of strategic stakeholders. Again, the assessment of emerging IT risks cannot be reduced to technical risks alone, but has to encompass a holistic view including multidisciplinary aspects of interrelated juridical, societal, economic and strategic issues.

Regulatory architectural patterns are emerging and could soon be advanced through standards bodies, establishing a repository of architectural patterns that address diverse compliance requirements. Continued advances, mapping, and relating contextual requirements to contextual solutions via frameworks will be necessary to advancing privacy assurance infrastructure. Research is needed for (among others): developing new approaches towards embedding privacy and trust/reputation features early on in the software lifecycle within system architectures (which are increasingly adopting either the Service Oriented Architecture paradigm or are at least service-based); balancing community-specific requirements and exhaustively analyzing user interaction habits; implementing usability guidelines; comprehensively understanding mobile environment ecosystems (including devices, operating systems, operators, network standards, software development kits and runtimes, server-side software, simulators and tools…) and leveraging rich mobile application capabilities (including dimensions for interoperability, security, pervasiveness, application management, data persistence and platform integration support…). PICOS can thus help the software industry to begin to develop safe and reliable services that protect personal information in on-line communities. In PICOS, frameworks, architectures, use-case models, and taxonomies will represent an emerging set of tools necessary to convincingly address many competing forces affecting information privacy.

The first obtained project results sketching PICOS' scope of different types of leisure and professional on-line communities are being used by ATOS to define the technological mobile environment from a client-side perspective considering the underlying requirements regarding trust, privacy and identity management as well as usability aspects. In addition, these outcomes provide generalized security platform requirements and finally legal and assurance issues, all of which will affect in different ways the work of ATOS in the platform prototype implementation phases, for instance, by clearly defining the scope of both functional and non-functional features which will demonstrate the value PICOS can bring to the chosen communities while ensuring the overall experience of the end users and the compliance with legal provisions, standards and assurance cases. PICOS is a strategic project in ATOS' R&D Agenda 2008-2011 and its results will undoubtedly enrich the portfolio of solutions that ATOS makes available for its customers while deepening our expertise in the key areas mentioned. Moreover, through the participation in NESSI[5], a European Technology Platform that is focused also in privacy, trust and security especially for web services, ATOS ORIGIN aims at establishing a mutually beneficial bidirectional relationship to PICOS.

PICOS Outcome

The results of PICOS will contribute to European competitiveness in several ways. The resulting platform will be a reference implementation of a state-of-the-art community–supporting identity management system. Its use by the industrial members of PICOS will create benefits and insights in the European IT and telecommunications industry beyond the scope of the project. By involving all stakeholders on the community value chain, PICOS will strengthen integrated European privacy and trust products. Europe's competitive advantage for trust in on-line applications and services will be strengthened.

Moreover, the PICOS 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 customers.

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. Society and communities will benefit from the privacy-enhancing technologies of PICOS, building trust in ICT, which will lead to more widespread use of ICT, while strengthening the ICT security industry. The PICOS outcome will also foster community-centered activities (both private/leisure and professional/commercial) in communities that cross national boundaries, by adopting an approach that supports interoperability.

Summarizing, PICOS and its partners are holding a wide spectrum of expertise for influencing strongly the future of the social networking landscape with regard to trust-enabling, privacy -enhancing identity management as well as the trustworthy and secure handling of content in social on-line and mobile communities. Considering the aforementioned identified possible gaps at technological and business levels, the W3C Workshop on the Future of Social Networking provides us an ideal platform for suggesting possible solutions for enhancing social networks and for discussing present and future of both emerging and increasing mobile trends. Such networks will need to be oriented towards a trustworthy and secure on-line experience for all the actors involved.

www.picos-project.eu

[5] http://www.nessi-europe.com

APPENDIX: SUGGESTED DISCUSSION TOPICS

In the following list we put further topics on discussion relevant in the scope of the W3C Workshop on the Future of Social Networking. A predictable development line of IT (including the Future Internet as an "Internet of Things" and "Internet of Services") will include, among others, factors such as:

- Ubiquitous, ambient, "infrastructureless" and pervasive computing in peer-to-peer modes, matched with ubiquitous and privacy-respecting service availability and a high degree of self-organization ("liveness properties"),
- device miniaturization and convergence, with the aim to turn devices into enablers of services by embodying service-oriented architecture (SOA) principles in embedded systems and to link collaborative devices to services (a paradigmatic example of this could be mobile online social networks which are likely to quickly expand in number of users and available services in the near future),
- higher availability of greater choice of bandwidths and wireless communications infrastructures,
- innovation in the field of multilateral security and greater interoperability between identity management and reputation-based systems, including portable reputation across different types of virtual communities (e.g., online/mobile, business/leisure) and market places,
- new methods for user-centered privacy management including the evolution of PETs enabling their seamless integration into open service-based and service-oriented architectures and ecosystems (a leap forward can also be envisaged in terms of their usability and acceptance by end-users),
- privacy evidence creation after execution, including audit by secure logging and the evolution of policies for contract representation beyond currently existing solutions (i.e., P3P),
- new services related to online communities, P2P networks and professional (social) networks, especially location-based services which pose complex privacy issues,
- integration of certifications, seals, privacy frameworks and architectures into new online systems (the ongoing work of standardization bodies such as ISO JTC 1 SC27 WG5 is likely to provide a sound basis in this direction).