

PROJECT FINAL REPORT

Grant Agreement number: 216483

Project acronym: PrimeLife

Project title: Privacy and Identity Management in Europe for Life

Funding Scheme: IP

Period covered: from March 1, 2008 to June 30, 2011

Name of the scientific representative of the project's co-ordinator¹, Title and Organisation:

Dr. Jan Camenisch, IBM Research GmbH

Tel: +41 44 724 8279

Fax: +41 44 724 8953

E-mail: jca@zurich.ibm.com

Project website address: <http://www.primelife.eu>

¹ Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

4.1 Final publishable summary report

Executive Summary

The vision of the PrimeLife project is to enable individuals in the information society to protect their privacy and retain control over their personal information, irrespective of the activities they are performing. Indeed, individuals and businesses are increasingly using social networking, online collaboration applications, mesh-ups of different services, and the Internet in general, for both private and business purposes. Unfortunately, the new information technologies hardly consider the privacy requirements of the individuals.

PrimeLife's Approach

PrimeLife's approach was threefold. First, PrimeLife picked up the results and technologies from the PRIME project and helped with their adoption in the real world by providing materials for standardization and education. Second, PrimeLife eliminated many of the remaining hurdles for large-scale adoption of these results by addressing user interfaces, policy languages, and infrastructural components. Third, PrimeLife provides a number of solutions for privacy, identity, and trust management in cases where protecting privacy by data minimization fails.

Privacy for Life – Beyond Data Minimization

PrimeLife provides privacy-enhancing solutions for Web 2.0 applications such as wikis, blogs, and social software that allow the users to assess the trustworthiness and privacy setting of information provider and to protect their own privacy when interacting with Internet sites such as social networks or blogs. For instance, the project has implemented and piloted its own social network that supports the user in defining who should and who should not have access to their data. Furthermore, PrimeLife provides a Privacy Dashboard as a browser extension that informs the user about the privacy settings of websites the users are interacting with.

PrimeLife has also investigated the long-term aspects of privacy and identity management and has identified life-time personal data management as a major issue. The project has made available a prototype of a tool that allows users to do just this, i.e., to define which other party should have the right to access that data under which conditions.

Enabling Privacy-Enhancing Privacy, Identity and Trust Management

PrimeLife has identified human-computer interaction, policy languages and access control technology as two main hurdles to overcome. To this end, the project has designed a policy language that fulfills requirements for privacy-enhancing access control and data management and embeds into the widely used XML and XACML frameworks. Also, the project's HCI experts have iterated on all the user-interfaces, improved them, and established guidelines for the design of interfaces for privacy-enhancing mechanisms. In addition to these two main hurdles, PrimeLife has identified a large number of other issues and provides solutions for many of them. These solutions include new mechanisms for privacy-enhancing access to databases, reputation management, the composition of services, mobile infrastructures, and a methodology for the economic valuation of identity and privacy management assets and capabilities of organizations.

Making Privacy Live

We believe that PrimeLife has made substantial steps towards privacy protection in the digital world. The project has published an enormous number of papers at international conferences, workshops, and in journals to disseminate its results to the scientific community. The project participants have given even more talks and keynote speeches to disseminate PrimeLife's results to the scientific community and, very successfully, to standardization bodies. Also, a book summarizing the results has been published and almost all prototypes are available as open source components ensuring sustainability of the results. In fact, we know already of a number of projects (including some EU-funded ones as well) that are or will be using results of the project. A less measurable, but very substantial, impact of the project is created by the workshops that the project has organized or participated in and which aimed at employing privacy-enhancing mechanisms in the real world. These workshops include political ones proclaiming that "privacy-by-design" must be employed in the future to concrete technical workshops discussing how to build privacy principles into browsers and social networks.

We are convinced and proud that PrimeLife helped Europe to come closer to offering citizens a protection of their rights of privacy in electronic interactions. This makes Europe unique in the world, particularly when comparing with the United States or Asia.

Project Context and Objectives

Individuals in today's information society want to safeguard their autonomy and retain control over their personal information for all on-line activities. Information technology requires users to disclose personal data in almost any kind of interaction performed online. Those information technologies do often not sufficiently consider the protection of users' interests in their private sphere. The web has been changing from a purely client-server-oriented paradigm to a more collaborative one. This collaborative character of the Internet makes the privacy situation more complex as multiple new kinds of interactions have emerged, e.g., users creating online content and sharing it with others or social interactions taking place online. In terms of the users' service delivery endpoints, the traditional web access device, the PC, is being gradually complemented or even replaced by mobile end-user platforms—mainly smartphones—which needs to be taken into consideration for addressing the privacy and identity management problems. With the increasing use of the Internet for business, government, and private purposes, personal data of users is released to and handled by an increasing set of parties, without it being clear to the user which parties hold their data in the end. Better transparency and data management for the user are to be provided.

This situation raises substantial new technical privacy challenges, namely protecting privacy in new Internet application paradigms, how to maintain life-long privacy, and how to provide secure access to online services. PrimeLife's goal is to provide solutions to those challenges and thereby to continue the work that has been started already in the PRIME project of the 6th Framework Programme.

The long-term nature of data storage on the Internet results in the major challenge of life-long protection of privacy and management of identities. This is addressed as one main goal of the project with impact to be expected in the mid term to long term.

PrimeLife's objectives relate to the abovementioned pervasiveness of the Web and Internet leading to a situation of those technologies and applications being relevant in all parts of peoples' lives. People use the web with an increasing pace throughout their daily lives. All of this creates challenges related to identity management and privacy, shaping one main objective of the PrimeLife project: enhancing privacy throughout lifetime and for complex situations. The work within the whole project is aligned around this. We tackle the associated challenges by different lines of work: Privacy in Life deals with privacy in complex and increasingly relevant real-life scenarios and sustainability of privacy. Basic Research builds a foundation of privacy-enhancing technologies (PETs) to be applied for supporting our efforts on the core challenges. Our Usability efforts make the various user-facing technologies usable, thus are a necessary condition for a successful agenda in the privacy research space. The work we do on Policies is required for formally expressing every party's (privacy) requirements and for allowing automated processing and user support. As a missing link towards deployment, our Infrastructure efforts are targeted at real-world deployment of privacy technologies which raises further challenges, e.g., the analyses of economic drivers, secure mobile devices, or complex service compositions. The aspects of privacy in peoples' areas of life and throughout their lives are addressed not only by a dedicated line of work tackling those, but particularly also through the concerted approach of technology research throughout the areas PrimeLife is doing research in.

Privacy in Life – Privacy in Complex Real-life Scenarios and Sustainability of Privacy

The pervasive nature of the Web and resulting applications clearly show some of the key issues PrimeLife tackles: How can users inject trust into their or others' content? How can the trustworthiness of content be assessed by other users? How can online collaborations be performed in a privacy-enhanced way? How can users be supported in their privacy management in social networking-like scenarios and be made aware of the associated privacy issues? How can we give users better overall control over their personal data in prominent scenarios? How can privacy protection be made sustainable through peoples' lives? All of those questions are closely related to privacy in the life of the average citizen today.

The line of work denoted "Privacy in Life" explores scenarios of content creation by users as well as social network scenarios and collaborative workspace scenarios with respect to privacy protection. In the area of user-generated content, a specific issue is to ensure that users can somehow inject trust into the content, e.g., through associating a claim of authorship or reviewership with relevant (certified) and typically non-identifying identity attributes attached. Such associated trust metadata can allow other users to make inferences on trust in the content, e.g., by judging the associated attributes. The key challenges for such a scenario are, on the one hand, foundational

challenges unrelated to privacy that need to be overcome as well as specific privacy-related challenges, e.g., to allow for the described functionality without associating the authors' or reviewers' identities openly to the content. Usability and policy issues are crucial for such scenarios. Trust models of different strength can be envisioned for this. The First Focal Prototype as well as the first versions on the non-focal demonstrators have shown key facets of trusted content scenarios.

For the area of social networks, better control over the data users provide to the social network needs to be put in place. As well, users need to be made aware of the threats to their privacy in social networks and similar applications. A particular goal in the second period was the Second Focal Demonstrator about social networks and collaborative workspaces. As an objective for Period 3 in this area, research as well as prototyping work in this area are further progressed in the areas with the highest potential impact.

In the third period, the project was to elaborate on sustainability aspects of privacy in identity management, that is, the *privacy throughout life* aspect. The third reporting period was to comprise the major design and implementation tasks related to the Third Focal Prototype.

The abstract objectives for the areas of work mentioned above were to develop technology and approaches for helping individuals to be better protected when acting in the mentioned scenarios.

Basic Research – Building the Foundation

The foundation for privacy protection in the envisioned scenarios and beyond is built through our basic research work. This work is, on the one hand, aligned with the challenges identified in our “Privacy in Life” work and other areas of our work and goes, on the other hand, beyond this and is intended to be generally applicable. The overall objective of the basic research is to develop mechanisms for the enhancement of trust and privacy in the information society. Parts of the research have a strong relation to the trusted content work in the “Privacy in Life” Activity. Research is performed in four distinct, but not independent, areas which are key areas strongly related to the overall project goals: Cryptography, user supporting tools, privacy of large data collections, and access control.

Usability – Making PETs Usable

As the title of this line of work already suggests, the objective of this Activity is to make privacy-enhancing technologies usable for the citizens. It is recognized that, without usability, even the best PETs do not deliver their features to the people. This activity is aimed at taking technologies from PrimeLife and elaborating on the user-facing aspects of those technologies. In particular, the activity is investigating mental models and metaphors for anonymous credential selection, develops user interfaces for transparency-enhancing tools and privacy policy management and display, including the development of privacy policy icons for more noticeably displaying policy components. Furthermore, the activity provides HCI guidance and implementation support for the Activity 1 prototype development as well as to other WPs that are developing user interfaces.

Policies – The Art of Formal Privacy Languages

In order to make our daily interactions on the Web more transparent to us, and in order for businesses to be able to better control the life cycle of data records they hold, PrimeLife created a system that allows the expression of Policies, constraints and requirements by both parties and helps to keep the data handling according to the initial promises made.

Many interactions over the Web require that privacy and data handling requirements be expressed in a formalized language, a policy language. Examples of such requirements extracted from our envisioned scenarios include trust requirements on content authorship, credential or, more generally, attribute requirements on a person or a service accessing another service, data handling requirements by users, and data handling offers of servers. All of those examples prominently appeared in the requirements study that we performed based on the scenarios of our “Privacy in Life” work of Activity 1. The goals of the policy efforts are a clean foundation of research results on top of which our policy model, architecture, language, and policy engine implementation is built.

Infrastructures – The Missing Link for Deployments

Today's information systems are highly distributed and interconnected. Thus, singular solutions for privacy issues, such as human-computer interaction or privacy-enhancing crypto schemas, have to be paired with an approach on the level of infrastructures in order to be successful. For real-world deployments, important aspects such as privacy-aware service integration, economic viability, secure end user devices etc. come into the play. Those need to deserve consideration when deploying privacy-enhancing technologies on a large scale in practice. PrimeLife's line of work in infrastructures is exactly looking at those aspects with a particular focus on the PrimeLife scenarios as well as generic applicability of PETs in the real world.

Privacy Live – Transferring Results into Practice

In addition to the technical activities, PrimeLife has a focus on transferring our results into practice. This is carried out as a line of work that picks up results from all technical areas of the project for dissemination. The instruments include the public Web site, workshops, summer schools, open source contributions, and standardization. All instruments are presently being employed. Two PrimeLife Summer Schools and multiple standardization workshops have been held to date with further ones coming up. Our interaction with standardisation in the relevant international bodies continues.

PrimeLife has taken an overall approach of tackling the challenges from a multidisciplinary perspective, taking technology as well as legal, social, and economic perspectives into account because we think that all those disciplines are required to succeed in the marketplace with practical solutions. The strength of PrimeLife is to have solid competences in all those areas and thus the ability to tackle problems from the envisioned interdisciplinary point of view.

PrimeLife has in its work built on the momentum and technology created by the predecessor project PRIME to address emerging challenges in the area of privacy and identity management to bring privacy and identity management to life. Bringing technology to life as a particular goal of PrimeLife, particularly through facilitating the adoption of our privacy technologies and not only our research on those. This has been achieved by dissemination of our results to the key target groups, with a particular focus on open source products we build, and work with standards bodies and policy makers.

Main S&T Results

In this section, we outline the main scientific and technology results of the project and show how they fit in the context outlined above and thereby meet our goals. We structure the discussion along the following areas: Social and collaborative internet, life-long privacy, foundational research, policies, infrastructure, and usability.

A main challenge of the diversity of today's online interactions is that there is no single technology or system that is a solution to all privacy problems. In the predecessor project PRIME we have been looking mainly at the problem of data minimization and provided a solution for this. Though, emerging paradigms such as the social web are not aligned with data minimization and therefore we have addressed the problem space of privacy-preserving identity management in a more comprehensive manner by looking at different areas of web interactions and classes of scenarios and applications and addressing issues at their different levels of abstraction. Quite different technological approaches needed to be applied for the different areas of online user interactions due to their different nature. Our results complement the results achieved in the area of data minimization in PRIME very well and partially build on those.

PrimeLife's approach tackled the privacy and identity management problem from various different points of view—foundational research to build a solid technology foundation, implementation of selected research results to show their practical feasibility, and building more comprehensive integrated prototypes to show the interplay of selected technologies. Certain aspects such as usability and policies were cross cutting and prominent in multiple of the research areas. Our approach created a mix of foundational research results, on the one hand, and practical results as well as prototypes, on the other hand. Thereby we could address major open problem areas of today's electronic interactions from a theoretical and practical approach and create considerable value for society at large.

We refer to the main freely available documents comprising our results by their identifier, e.g., D1.2.3. All such documents can easily be retrieved from <http://www.primelife.eu/results/documents>. For open source results we provide direct web links. A summary of project is given by the book that has been published about the project results.²

The Social and User-driven Internet

The Internet has become a social medium within the recent years and PrimeLife had anticipated this strong move already in its inception phase and allocated major work efforts towards solving the privacy challenges inherent to such a social medium. What we denote as the social Internet is the availability of a plethora of web-based services in which users make contributions of content online and provide personal data to services, where both content and data become available to a (restricted) set of users of such web-based services or even the public. Examples for such services are social networks, wikis, or discussion fora. We next provide the reader with an overview of our results in the field of the social Internet.

Trust in User-generated Content

One main problem related to user-created content on the Internet, such as community-created Wiki pages, is the problem of the assessment of trustworthiness of the content contained in those through users. As people increasingly rely on such community-created information for both business and personal purposes, we have investigated this area. The problem is how to add trust to content such that it can be an indicator for content quality perceived by content recipients. Such trust can, for example, be established by information about the author, ideally without identifying information, or by ratings on the content and knowledge about the rating parties.

We showed how one can *inject trust* into user-generated content using the example of a blog by adding meta information about the content creators (D1.1.2). We found through user studies on the prototype that, while we have been able to define technical solutions to this problem, the key issue of having trust meta information contributed by users is to incentivize the users to contribute such. Driven by this finding, we designed a *privacy-preserving incentive scheme* to resolve this issue. The scheme uses the Identity Mixer anonymous credential scheme to allow users to anonymously perform reviews of content created by other users while earning credit points as incentives that are of some real-world value to them (D1.3.3).

We performed a user study on privacy implications of user reputation and found that stronger privacy properties can mitigate issues of non-participation of users in such schemes. Motivated by this result, we designed protocols

² Jan Camenisch, Kai Rannenberg, Simone Fischer-Hübner (eds.): "Privacy and Identity Management for Life", Springer Verlag, 2011.

and built a prototype for a *privacy-enhanced reputation scheme* for Wikis, again based on the Identity Mixer anonymous credential system as a strong technical foundation. The scheme allows for both author and content reputation in Wikis where users can contribute reputation ratings of wiki pages and other users without revealing identifying information or their ratings being linkable. The prototype implementing this scheme has been integrated with the widely-deployed MediaWiki system by means of an extension to it and made available as open source offering³. (D1.3.3)

The abovementioned solutions have been implemented as prototypes to show their practical applicability, particularly in widely-used products such as MediaWiki. Technology wise we have built our prototypes based on deployed web technologies on which we had performed an analysis beforehand (D1.1.1). At multiple points we had to overcome the integration of new technologies, such as anonymous credential systems, with standard and widely-deployed web technologies and found such integration to be workable in practice. The schemes that require anonymous credentials are dependent on third-party-issued credentials, which is a strong assumption on the environment. Thus, such schemes are dependent on and can be a driver for a deployment of credential systems such as Identity Mixer or U-Prove once users see the value. Further studies with the prototypes have given us insight into the need of the abovementioned incentive scheme for motivating users to contribute their ratings. Our incentive scheme and reputation scheme can be combined to resolve this issue.

In addition to our theory and technology development, we have performed evaluations of our prototypes that have partially driven our ongoing work as well as further user studies. The studies investigate trust perception of users, e.g., for displaying search engine results, privacy-preserving reputation, and users' assessment of anonymous reputation to uncover how content recipients perceive the quality of content in the light of the reputation of the content creator. (D1.3.3)

Privacy for Social Software

Social networks have been gaining major traction in the recent years and are major aggregation points of personal data users release voluntarily to the system to benefit from the offered social functionality. A major requirement for user privacy is that users be able to control the dissemination of their data to other social network users or the public, that is, to have selective access control to user profile data and other user-generated content in place. Particularly, users are also able to segregate the target audiences of content related to them. Today's social network platforms often do not allow users to make such settings or it is not easy enough to do so from a perspective of usability or integration into the users' workflow. In this line of work we have done a requirement analysis of privacy-enhancing access control for social networks and collaborative workspaces which acted as a basis for further research and prototypes being developed.

As major result in the area of *privacy-enhanced social networks*, PrimeLife has extended the premier open source social network Elgg with multiple privacy-enhancing features. The concept of audience segregation, that is, to differentiate between target audiences for personal data items, is implicitly realized by people in their daily "offline" life. We have transferred this concept into the electronic world and enhanced the Elgg social network with an implementation of the audience segregation concept (D1.2.1, D1.2.2, D1.3.3). Users can now act under different "faces" and thereby differentiate between the intended audiences. Another facet of better access control to profile data is the definition of access policies on a fine-granular level, e.g., by assigning rights to individual users or groups. The strength of our implementation is that it features an easy-to-use user interface for such access control policy definition which is integrated in the standard workflows of the social network. We also investigated an experimental feature for implementing user consent to uploaded materials if a user's data is concerned, as is frequently the case with photographs containing friends being shared in social networks. Another example for a user-supporting feature of the prototype is a fading of relationships between users with no interaction over long time. All mentioned features need to be implemented by the social network platform; thereby their support needs to be gained for ensuring a proliferation of such features in practice. Our prototyping work was in line with related theory research on privacy in social networks. One specific result worth mentioning is a paper on Facebook's "Like"-button analyzing the tracking of users, be it Facebook members or other users.

In addition to the provider-implemented access control for social networks as outlined above, we have realized an idea requiring no support by the social network provider for its realization: We leverage the available "Web of Trust" through which many of today's Internet users' public keys are certified by other users. Based on this readily-available community-driven and non-centralized public key infrastructure, we have built a browser-based

³ <http://www.primelife.eu/results/opensource/57-mediawiki-reputation-extension>

encryption tool that allows a user to encrypt text fields on web pages towards a selectable audience.⁴ (D1.2.1, D1.2.2, D1.3.3) This ensures that the server on which the content of the text field is stored need not be trusted as access control is realized through encryption with the user-selected keys and trust in the Web of Trust certification of the keys. This is a much stronger trust model than for the above approach. The results are orthogonal to the abovementioned work on social networks, but can be integrated in terms of deployment. As a complementary result, we have elaborated how social networks can be exploited to facilitate key certification through the Web of Trust which may open up this certification infrastructure also to less technology-oriented Internet users.

PrimeLife has also investigated—as another representative of social software—the area of privacy-enhanced access control in collaborative workspaces, such as online fora. In this area, we have taken an approach with more infrastructure requirements, namely the availability of anonymous credential systems. The prototype shows how users can define access control policies for their forum entries which interested readers can fulfill using appropriate Identity Mixer credentials.⁵ (D1.2.1, D1.2.2, D1.3.3) This approach realizes audience segregation for the to-be-protected content based on the access control policy being defined. We have shown that such an approach is workable, though, deployment is harder to achieve due to the requirements of a credential infrastructure being in place.

All three prototypes described above have been made available as open source products under the links as indicated. Regarding deployment, the assumptions on reliance on external parties and required infrastructure cover a broad spectrum: Deployment through service provider, use of Web of Trust certification, and availability of a credential certification infrastructure. The approaches with the least assumptions have the most realistic chance of short-term and mid-term real-world deployment. Major non-technical issues that may influence deployment are business models and legal aspects, e.g., the use of encryption in such services. The different approaches also have demonstrated the assumption of different trust models, ranging from a fully-trusted platform provider to no trust requirements in the platform provider.

Foundational Research

We next outline our foundational research results that provide the foundation of privacy throughout users' lives. Parts of the results have been implemented to show practical applicability of them and much of the source code been used made available to the community as open source. An overview of the findings as well as pointers to our scientific papers are reported in our periodic research reports D2.1.1, D2.3.1, and D2.4.1.

Cryptography for Privacy

A major basic research effort has been carried out in the area of cryptographic protocols for privacy. The main advantage of cryptographic solutions are the reduction of trust assumptions in other parties and the possibility of reducing information disseminated to other parties compared to a setup without cryptography. We covered multiple areas of research where we could substantially progress the state of the art.

One main theme of theoretical cryptography research was *anonymous credential systems*. Such systems are the best known means for authenticating users based on certified attributes or pseudonyms and allow for data minimization by revealing exactly the information as needed in a transaction. Particularly, transactions can be unlinkable from each other if this is required. We have found protocols which allow for more efficient encoding of certain classes of attributes which is important in the light of real-world deployments and credentials with multiple attributes. As one of the sub-aspects relevant for credentials, we have developed more efficient revocation schemes which is crucial in the light of large-scale deployments of credential schemes, e.g., in the context of eID schemes. An interesting technical contribution was a new method of partially releasing data of a credential, namely an approach for efficient set membership proofs, as a cryptographic building block for credential systems. As one breakthrough, we have shown how to obtain delegatable credential systems while retaining the full privacy and security properties. By this, we have solved a long-open problem in cryptography.

As a cryptographic application of credential systems, we have developed a protocol that allows two parties to establish a shared secret, e.g., a secret key for message encryption, if and only if both parties hold credentials that

⁴ <http://www.primelife.eu/results/opensource/65-scramble>

⁵ <http://www.primelife.eu/results/opensource/72-phpbb-peac>

fulfill a given policy. The only thing learned by the parties about the other party is that it fulfills the policy. Nothing is learnt in case the protocol does not succeed. Such a protocol is interesting in the context of previously-unknown parties on the Internet engaging in a communication relation.

At a theoretical level, we could prove that there exist efficiency limitations in the cryptographic protocols, so called zero-knowledge proofs, underlying our credential system and many other cryptographic primitives. As a practically-exploitable result, we have come up with a protocol composition framework which allows for a much simplified and modular composition of zero-knowledge proof protocols. This is particularly important for the Identity Mixer protocols.

As another key contribution we have realized an encryption scheme which has security properties required when one wants to back up secret data through encryption. Such a scheme is a required building block for infrastructure for credential systems that would allow users to back up their secret key.

As a building block for protocols that involve a trusted third party optimistically, that is, only in case a conflict needs to be resolved, we have developed a protocol that ensures that the trusted third party cannot discriminate between parties for which it gets involved in. Such third parties are denoted *oblivious third parties*. This strengthens the model in which cryptographic protocols can be executed by further reducing trust assumptions on the third party.

We made major contributions in the area of *private service access*. The setting here is that a user can access a service in an unobservable manner, that is, the service will not know whether which part of the service was accessed, e.g., which record of a DNA database or patent database or which user profile of a social network provider has been accessed. A method for achieving such private service access has been proposed. A method that can be seen as an extension to this basic setting has been found. It allows users to access content in an unobservable manner while allowing only users who have the necessary access credentials to decrypt such records. As a further natural extension of the model, we have a protocol allowing to charge a price for a record accessed in a private manner as outlined before. This makes the approach applicable to DNA or patent databases or other valuable resources where it is important that the user does not disclose information on the record being accessed.

Fair exchange of digital content is an everyday problem. Cryptographic fair exchange protocols ensure that there is no trust required in the parties taking part in a protocol for providing their input to the exchange, but ensure that an exchange of the digital goods takes place fairly or not at all. Thus, no party can betray the other by receiving the good of the other and not providing its own. Such mechanism is not important in the traditional setting of e-commerce, but rather when parties who do not know each other engage in exchange transactions over an electronic communication network. We have found a fair exchange protocol for large files in a peer-to-peer setting where either two files are exchanged for each other or a file against a payment. Another contribution is a protocol for fair exchange of one of a list of electronic goods against a payment without the seller of the goods learning which one was accessed. This is in a similar setting as private service access.

In order to obtain security of services and full user accountability, binding of users to a device helps resolve some of the issues. Biometry is one way of achieving this, possibly as one of a set of authentication factors, e.g., in addition to a user-known secret. We have obtained new on-card fingerprint matching algorithms and software integration. Such technology is an enabler for service security in future service infrastructures. Together with our developments on Trusted Execution Environments (TEEs) for mobile phones, this is a basis for portable digital ids with biometric access control.

Related to anonymous credential systems, we have developed approaches for securing a user's credentials by realizing the concept of *trusted wallets*. We have looked at implementing credentials on standard JavaCard smart cards which can be considered a breakthrough result in the system area. It realizes for the first time a use of credentials where the private key is secured from potential attacks from the host such as attacks through malware. This is a particularly important result in the light of employing credentials in the context of eID cards. Credentials on smart cards have been employed in a scenario where the smart card is implemented as a secure microSD card running in an Android-based smartphone for an e-petition scenario.

We have elaborated on a high-level architecture for secure wallets comprising different layers of protection: operating system; wallet software, e.g., in virtualized compartment; hardware token. Based on the results, we have focussed this line of work on the field of smart cards in different form factors as one key class of hardware tokens. Virtualization is a commodity today and orthogonal to obtain secure input and output user interfaces. Of mention here is also our work on Trusted Execution Environments (TEEs) for realizing secure compartments on mobile phones.

Reputation

Reputation can be seen as one of the key factors influencing decisions of any kind, also on which parties to interact with online. A *reputation system* that protects the privacy of its users has been designed, which fulfills the new protection goals of liveliness and fairness while assessing privacy based on information-theoretic measures. Thus, the system balances the security and privacy requirements of the users of the reputation system and, that way, it achieves multilateral security. Another reputation system was designed specifically to integrate with the semantic web, again offering multilateral security. Both systems have been implemented as prototypes. One overarching research aspect in this area was the interoperability of reputation systems with other systems, which is crucial for any real-world deployment.

Privacy Awareness

Based on studies we examined from the field of e-commerce, it became clear that a privacy paradox exists, that is, a discrepancy between users' stated attitudes and their actual behavior with respect to personal data handling exists. This paradox seems to be present equally in web communities and social networks, with a possible additional factor being a gap between intended disclosure groups for data and the actual groups. The project suggests supporting privacy awareness in such situations to remind users about their intentions and make those explicit. We have performed online user studies on privacy awareness of users as well as the impact of privacy awareness information on user behaviour. We found that the perception of being private decreases with the availability of privacy awareness information, e.g., by showing the audience of to-be-released information in an explicit way. We showed how to use privacy awareness technology in practice by a privacy awareness extension to phpBB.⁶

Transparency Tools

Transparency is one of the basic requirements that the European Data Protection Directive imposes for electronic transactions. Based on a classification of aspects of transparency tools and an overview of such, PrimeLife has developed a *secure logging* method that allows users to be able to reconstruct a trace of data disclosures across multiple data controllers. Arbitrarily complex downstream data release paths are planned to be supported by the approach in the future. The key novelty is that our log scheme is, unlike previous schemes in this domain, privacy preserving. The trust model is such that it assumes that data controllers apply the secure logging algorithms as specified. The core of the system has been implemented and shown to be workable. This result can be combined with our prototype on data tracking to obtain a stronger data tracking mechanism.

Privacy for Large Data Sets

Today's businesses and web site operators process large data sets of user data with an increasing pace and increasing sophistication. Such large data sets are often released to third parties for processing or secondary use. Due to the importance of this part of data management, we have investigated the assessment of risk of data exposure through metrics and new theory and mechanisms for guaranteeing specified privacy properties when releasing data to third parties.

Privacy metrics are a prime tool for assessing the risk of unintentional exposure of information when handling large data collections. We have elaborated on such *privacy metrics* and *theory of privacy* as the foundation for methods for the protection of privacy in large data collections, based on quantitative assessment of privacy and risk. We investigated the problem of user support for the appropriate choice of anonymization techniques to reduce the risk of disclosure. We furthermore elaborated a unifying framework for combining metrics like *k*-anonymity, *l*-diversity, or *t*-closeness. Although those metrics measure different aspects of privacy like identity disclosure risk and different aspects of attribute disclosure risk, the goal is to obtain a single metric that allows for taking an integrated look at all those metrics in an optimization problem. We take an information-theoretic approach and express the three metrics as contribution to information.

⁶ <http://www.primelife.eu/results/opensource/59-phpbb-pam>

In the area of *enforcement of data privacy*, results were obtained in representing privacy constraints for relational databases as access privileges to parts of a distributed relational schema. This helps protect privacy in scenarios where different sources of personal data may be integrated and thereby increase the risk of undesired access. Another contribution addresses the enforcement of privacy constraints that express sets of attributes that must not be accessible together for relational data held by a third-party server. The approach taken is a fragmentation of the data schema such that each fragment stores only attributes compliant with the constraints. Efficiency is reached by considering the query profile in the computation of the fragmentation. A logical extension of this work is a scenario where users may hold confidential data on a lightweight trusted device locally which is involved in query processing. For such a scenario the fragmentation algorithm can optimize for keeping local storage on the device minimal. Many use cases such as application testing and support require real-world-like data sets to be available. This is a classical and practically important case of secondary use of large sets of user data. Though, data can often not be used as is because this would violate the privacy policy agreed with the users. We have looked at the resulting dilemma between anonymity and utility of data and investigated approaches for sanitizing data to obtain data sets useful for secondary use while complying with the agreed data handling.

Further contributions to privacy-compliant data publishing have been made through balancing confidentiality constraints and visibility requirements of the involved actors by data fragmentation, i.e., splitting sensitive associations while ensuring that visibility requirements are fulfilled. For scenarios where large datasets are released, we provide an approach for estimating the inference risk from such data to avoid leakage of confidential information. A new metric, based on information theory, to estimate such risk has been proposed.

One result that is specifically targeted at solving efficiency issues of privacy approaches in the outsourced data scenario builds on a so-called shuffling operation on an index structure over encrypted data by the storage provider to avoid it learning the accesses to the data realized by the user in addition to mere data confidentiality. The approach introduces little performance overhead and thus proves to be useful for practical applications.

Access Control

In today's Internet, data of users are often disseminated by a first recipient party, such as a service provider, to further parties, also for secondary use. Therefore, key aspects of data management are *dissemination control* and *secondary usage* of data of users, particularly also of contextual data such as location which is increasingly used for providing value added services.

The following results all improve on the dissemination control and secondary use of data of users with strong consideration of the widely-used XML framework for expressing and processing data. We have first studied how secondary use restrictions are expressed within standard policy languages such as XACML and what is missing, e.g., for policy composition. We have proposed a method to allow users to precisely specify to which parties location data may be disclosed based on policies. As an orthogonal means of protection, due to location being highly-sensitive data and thus requiring advanced protection, we have developed a mechanism that helps preserve location privacy by perturbing location information in various ways, following the user's privacy preferences expressed in a simple way. For dissemination control of user data contained in XML documents, we have proposed an approach for realizing selective disclosure of information in XML documents by filtering out data that is to be kept confidential according to an XACML policy and an ontology. The ontology allows for regulating disclosure using semantics expressed in the ontology and not only XML schema constraints.

A different setting we have considered for access control to users' data is what we call the *data outsourcing scenario*, that is, the scenario where personal data of users is stored on external servers which are trusted to perform operations on data as expected, but who are assumed to be honest-but-curious parties, that is, parties that are interested in learning the data. As the cloud storage model of cheap storage with few security guarantees and weak trust model becomes increasingly important, we have studied the problem of maintaining proper access to outsourced data by legitimate parties, but preventing the server from learning the data. Our solutions are based on cryptographic enforcement of the access control policy, in contrast to the usual enforcement by the policy enforcement component of the trusted data holder. This is a much stronger trust model than the standard model, by making fewer assumptions on the storage provider. One solution realizes a cryptographic enforcement of authorization policies through encryption and hierarchical key derivation. The problem with this approach is that still the authorization policy gets exposed through the cryptographic key derivation. An extension to the model fixes this exposure of the authorization policy. A different approach to solve the same data outsourcing problem has been proposed based on encrypting data with different keys and communicating these to the users. The challenge

here is that, because users have access rights to different data, many encryption keys may result for each user. The goal was to minimize the number of keys to be handed out to users to make the approach scalable and efficient. The solution is based on linear programs and heuristics for the key minimization problem. An extension to the method addresses the problem of efficient key updates for scenarios where data changes dynamically. Another approach we have investigated for data confidentiality in the outsourcing scenario allows a user to share a resource with other peers in the network by means of external servers while ensuring confidentiality of the resource and their content with respect to the servers themselves.

A special case of the data outsourcing scenario is when biometric data is stored on a server to be used in biometric user authorization. Here, the storage provider is an information infrastructure which we want to prevent from learning the biometric data in plain form. An approach was proposed that achieves such protection through a new way of registering and verifying the biometric readings. Another proposed method uses homomorphic encryption to hide the biometry from the server and the network infrastructure.

In certain cases of access control, the information about a user's presence when an operation is being performed could be exploited in the access control policies. We have proposed approaches that allow detection of presence of users and to exploit such contextual information for access control. This is orthogonal to the above results in access control and can increase the power of access control.

Implementation of Data Minimizing Interactions

The *Identity Mixer* library that has been created in PRIME has been further developed. New features have been added, the code quality has been improved, and a substantial effort has been spent to create documentation for the API of the library. The library implements the world's most advanced anonymous credential system that allows for anonymous authentication using attributes certified in credentials (privacy-friendly certificates). Such a credential library is a key building block for realizing data minimizing interactions. It allows for performing transactions with releasing exactly the amount of information required (and requested by) the interaction partner. As a specific feature, an anonymous credential system like Identity Mixer can allow for user accountability in such anonymous interactions, that is, the user's identity can be recoverable, e.g., in the case of a severe violation of agreed terms of service. The open source code⁷ of the Identity Mixer library will be maintained after the PrimeLife project and is already being used in a number of other projects. The Identity Mixer library has been used by multiple prototypes within PrimeLife, such as in the implementations of our privacy-enhanced reputation and incentive schemes. See D2.1.1, D2.3.1, and D2.4.1 for related scientific research papers.

Policy Language and Engine

PrimeLife considers policies as being of premier importance for the protection of data and the privacy of users in today's information systems. Particularly, proper policy-based data protection is one cornerstone of life-long privacy. Policies are used to govern access to resources while following the data minimizing principle, to agree on data flows and data handling practices, and to enforce the latter. For this reason, we have been doing extensive theoretical and practical research in this area, starting from policy requirements, over research on models and languages, to an implementation of a powerful policy engine for privacy-preserving identity management.

As first result in our policy research area, we have collected a comprehensive set of *requirements for a future policy system* being capable of expressing access control and data handling aspects. (D5.1.1) Based on those requirements we have designed a policy language combining elements from both the access control and data handling domain, denoted *PrimeLife Policy Language (PPL)*. (D5.3.4)

A particular *access control* feature of PPL is that it is able to express the semantics of anonymous credentials and thereby a policy engine implementing it is a suitable building block for systems featuring privacy-preserving access control through minimizing the amount of data released in each transaction being performed. The language is capable of expressing access control requirements in the full continuum from transactions with anonymous users to transactions with fully identified users. As a special feature, user accountability can be ensured even in transactions

⁷ <http://www.primelife.eu/results/opensource/55-identity-mixer>
<http://prime.inf.tu-dresden.de/idemix/>
<http://idemix.wordpress.com/>

where a user remains anonymous, such that a user's identifying attributes can be recovered with the help of a trusted party under well-defined circumstances. The access control part of the language is technology agnostic, which makes the language applicable for a plurality of possible authentication technologies, with anonymous credentials being the most complex and powerful one. We have adopted the paradigm of a card as a collection of (certified) attributes stated by an issuer and allow for multiple such cards being used by a user to fulfill a single policy request of a service it wants to access. This gives the approach the expressive power that is required in real-world interactions where a request does not necessarily comprise only data from a single issuer.

Regarding *data handling*, the language allows users to express their data handling preferences as well as data controllers to express their data handling promises. Both those can be matched before a data release transaction takes place and result in a concrete policy to be enforced for the data to be released. The underlying policy model has been designed for supporting service compositions of arbitrary depth and to have enforcement take place at every party in such a service composition. A key feature for such compositions is the capability of downstream usage control, this being the agreement on policies for further data recipients that match the user's preferences and enforcing such constraints for all disclosures of user data along the services chain. The complexity coming in from composed services is that the policy exposed to a user may be a composed policy, composed of multiple policies of back-end data recipients. One important part of our data handling policies are obligations which specify operations on data and how to trigger them, e.g., time-based deletion or notification of users when data are further released to downstream parties in a services chain. We have designed a powerful language and a matching algorithm as part of our data handling policy language and engine.

Sharing of data by the first service provider a user releases data to is used virtually everywhere in today's web as data sharing is the driver behind many business models, but also for achieving cost reductions through outsourcing. PPL adds better control, automation, and privacy to such scenarios.

We have built an implementation of PPL, the PrimeLife policy engine, and used it in our prototyping activities to show its practical applicability. As important step towards technology adoption, we have released a core part of our policy engine that is related to privacy-enhanced access control policy matching. Such a component is a necessary building block when deploying an anonymous credential system in a practical environment. The full specification of the PrimeLife Policy Language has been made available as an open specification to make our results available on a broader basis. We have started to standardize the core parts of our language that are needed in order to take a first step in the deployment of practical privacy-preserving identity management systems. Concretely, this concerns the data format for releasing data in a data-minimizing way.

Related to the definition and implementation of PPL, foundational research was conducted in the policy space, among it the following (D5.2.3):

As an extension of PPL, we have defined a model for *disclosure policies* to regulate how access control policies for a party's services may be communicated to clients. As the client-side counterpart, which is, due to higher protection requirements and human attendance, not a fully symmetric situation, we have found a solution for *regulating disclosure of credentials* of a user. It allows a user to specify the sensitivity of credentials at a fine-granular level and automated enforcement of this during an interaction with a service provider.

Context-aware policies allow for an exploitation of context information such as location to influence how and when a policy should be enforced. This is important as the increasing availability of users' context information makes it possible to have context-sensitive services.

Using *policy spaces* we investigated how to regulate exceptions to policies, e.g., for emergency care in medical settings. With this approach we strike a balance between the rigorous operation of traditional access control on the one hand and emergency care requirements on the other hand. The goal here is limiting break-the-glass accesses, that is, emergency accesses by normally unauthorized persons, by classifying a subset of these access requests as abuses and defining policies for regulating those.

Further results have been obtained in the area of specification and enforcement of *privacy constraints on distributed data*. Often data are stored at multiple parties and for delivering a service, different parts of the data need to be seen by different parties. This is a problem of distributed authorization for and we have provided a solution for this.

As complement to our technical work we also investigated the policy area from a legal point of view, by extracting requirements for and guiding our technical work in this area. We looked at legal aspects related to the management of personal data with a focus on transparency and the purpose binding which influenced our policy model and PPL towards strong legal compliance with European data protection legislation. Also in the legal domain, we looked at for which kinds of transactions personal data are necessary, based on scenarios. This resulted in a differentiation for

transactions of web shops that may act as guide for practitioners in implementing data minimization in real e-commerce scenarios. We looked, from a legal perspective, at multi-level privacy policies, that is, policies that allow users to view different levels of abstraction of a policy to ease its understanding.

As a simplified yet effective means for displaying policies for email communication the project co-developed, jointly with Stanford University, the *Privicons* which are simple icons targeted at the end user to indicate data handling requirements in email communication.

legal requirements for privacy policies; basis for technology; technically-supported privacy policies; implement legal requirements through sticky policies; authorizations, obligations; analyzed existing models and languages

In the legal area we defined a methodology for analyzing existing provisions on data handling, e.g., privacy policies, regulations, and use cases and contributed to the policy language development efforts to ensure their legal compliance.

Identity, Trust, and Privacy Management on Mobile Devices

Starting from the concept of security of service, that is, a holistic, end-to-end, view of services security, we have looked at how infrastructure can contribute to realizing such end-to-end security requirements. Based on our analysis of market trends, we have focused on the enormous growth market of mobile devices and their use as infrastructure elements for delivering secure services to the users. In order to obtain secure services, mobile devices offering substantially higher security than deployed today, are needed. Multiple technologies such as smart cards, SIM cards, or secure microSD cards were assessed and compared with each other in the context of their use within mobile devices for obtaining a secure platform as key building block for secure services.

A focus was on using the concept of a Trusted Base to obtain better security of a platform by combining hardware and software security. The Trusted Base acts as a trust anchor on which further elements can be built for obtaining a secure environment in which a user can safely manage her identities and interact with her identity service provider. Particular aspects are security of private keys and secure input and output devices that cannot be compromised by malware. We analyzed available technologies for hardening mobile devices and at the potential future development for the dynamic creation of mobile services (D6.3.1). A prototype based on an Android mobile phone was built with a secure microSD card as Trusted Base (D6.2.2). The system is a first step towards obtaining a Trusted Execution Environment (TEE) where a user can perform identity management-related operations securely and showcased how one can get around main security issues coming from attacks on the computing platform and operating system. The prototype was employed for the specific application case of acting as the user's data management device for privacy-enhanced service compositions as explained further below. Major steps forward were made in the standardization of such Trusted Execution Environments within the Global Platform Alliance.

Enabling Privacy for Composed Services

PrimeLife has investigated service infrastructures that provide services to users while requiring personal data of users to do so. Our goals were to achieve a secure, convenient, and legally-compliant infrastructure for handling users' data in complex, multi-layered service compositions. In such service compositions (parts of) a service are provided by chains of service providers and user data flow along those chains as needed for the services. The dynamic binding of services may depend on the user's privacy preferences as data may only be passed from one service provider to another one if it agrees to handle the data following the user's preferences. Thus, policy composition is a key enabler for such dynamic service compositions. Both those aspects have driven our work in this area.

Our research results focus on an understanding of policy-driven privacy and data management in cross-domain service compositions. A framework for privacy and life cycle of personal data in service composition has been proposed that describes how the privacy aspects of complex service compositions can be addressed with the policies based on the PrimeLife Policy Language (PPL) (D6.3.2). The framework identifies patterns for enabling the use of policies in SOAs and thus may be a driver for real-world adoption of our technologies. As policy conflicts, that is, a composed policy for a service is not matching a user's preferences for her data, are a major issue in complex service composition scenarios, we have investigated conflict resolution in policy matching, with a particular focus on finding the root causes for such mismatches and thereby assisting policy management and future

user interfaces related to matching of data handling policies. Overall, our technical results in the service composition area leverage and integrate with our policy technology described earlier as a part of the solution. On the legal side we elaborated on legal aspects of data management in service compositions and particularly guided the development of our framework and prototype from a legal perspective.

A prototype for a concrete scenario of a service composition helped us validate our theoretical results and shows how user privacy can be retained in dynamic cross-domain service compositions (H6.3.3). The prototype was partly built based on the commercial Business Process Management (BPM) offerings BizTalk and NetWeaver and thereby shows the practicability of our approach in real-world technology settings. Another practically interesting result is the possible involvement of users through their trusted mobile device into service compositions to allow for policy adjustment in order to unblock a composition of a blocked service (D6.2.2). This approach of secure front-end to back-end interaction shows a trade-off between privacy requirements of users and feasibility of a composition being possible from a policy perspective, given the user consents to such adjustment of preferences. This is particularly interesting for services which comprise complex compositions and substantial risk of getting “locked” due to policy mismatches while having large potential value to the user such that weakening the policy for this service instance may be acceptable.

User Interfaces for Identity, Trust and Privacy

It is well known that usability is one of the main aspects that may inhibit or drive the adoption of security technologies. PrimeLife has addressed usability issues with a strong focus on the user and user studies we have performed. Our usability work has provided support, through user interface design, user evaluations, and user interface implementation for prototyping activities that have been performed throughout the project. The goal of the work was to find usable and understandable user interface paradigms for our identity management technologies.

General research on user interfaces for privacy-enhancing identity management has been performed. Results have been obtained in users’ comprehension and mental model of privacy-enhancing identity management through a combination of literature studies and expert evaluations of technologies. Through online studies we have investigated the conditions that influence technology acceptance and are preconditions for adoption of technologies. New user interface paradigms and metaphors for privacy-enhancing identity management have been investigated, also for virtual community applications. A collection of commonly-reappearing user interface patterns has been proposed. (D4.1.1, D4.1.5)

Substantial progress was made in the area of *trust and assurance* user interfaces with the goal of producing a tool to users for assessing the trustworthiness of service providers in terms of privacy protection and business reliability in a usable way, based on information from trusted parties and dynamically-generated assurance claims of the service provider’s data processing system. (D4.2.1) For the design of the trust evaluation function, we have taken the social, technical, organizational, and user interface aspects of the problem space into consideration. Our laboratory evaluation has shown that users do appreciate and understand such functionality. A cultural comparison study on the trust evaluation function has been conducted to shed light on different perception and acceptance of trust assessment depending on differences in culture.

We performed research in the area of online functions to give users the possibility of exercising their rights given to them by the European data protection legislation, e.g., updating personal data, blocking the processing of data, or requesting deletion of data. The basic underlying technical and user interface concepts have been elaborated and a tool has been implemented that allows a user to view their complete data track and perform abovementioned access to their data through a single tool. (D4.2.2) This can substantially enhance transparency and gives users the possibility to actively perform desired actions on their data. A fully-functional prototype of such transparency functionality has been built based on iteratively-evaluated and improved mock-ups.

Another transparency-enhancing function, specifically for virtual community users, was designed. It allows users of such communities, e.g., social networks, to be able to consent to the publication of data by others that affect such user. This carries well-known provisions of European data protection legislation over also to be applied to users who process personal data of other users. A legal analysis has been performed on the transparency functions which guided the technical work.

As a natural complement to our technical work on policies, we have elaborated on user interface aspects related to the presentation and administration of policies. For the access control part of the policy language we have elaborated concepts for a user-friendly selection of data based on credentials to obtain a valid assignment for a

policy of a service provider. Different metaphors have been looked at, particularly the card metaphor. We have further progressed it towards supporting the selection of partial information from a card and combining multiple cards (and the underlying credentials) in a single interaction. The work is well aligned with anonymous credential technology for privacy-enhanced data release, developed in the PRIME and PrimeLife projects. The main problems of cards as a user-facing concept were found and fixed in an iterative approach. Further concepts were tested as well. This work has led to a major progress in the knowledge on identity selection (policy fulfillment). (D4.3.1, D4.3.2)

For complementing our data handling policy efforts, we have worked on on-the-fly definition and change of data handling preferences during the context of interactions with service providers. Mismatches of a user's preferences with the service provider's policy are presented in a multi-level structure with increasing detail and the option of adapting the user preferences on the fly. As an additional level of data handling policy representation, a simple icon representation of key aspects of data handling policies has been defined and tested in an intercultural comparison study with participants from northern Europe and China.

In the course of user interface work related to the project's technologies we have published a collection of HCI patterns for the PETs we use (D4.1.3). For evaluations of usability of PETs, we have proposed PET-USES (Privacy-Enhancing Technology Users' Self-Estimation Scale), a questionnaire enabling users to evaluate PETs (D4.1.5).

The approach that has been employed in the user interface efforts was a combination of literature research, laboratory user evaluations, expert evaluations, and online user studies of mock-ups or systems. For use within the project, the well-known tool of personas has been used for capturing and communicating requirements for the technology-building and evaluation process and for facilitating communication between technical and non-technical team members. European data protection legislation was considered for our tools and interfaces for supporting users in order to ensure their legal compliance.

We have summarized the lessons we have learnt during the project in the areas of PET user interface design and evaluation (D4.1.6) which is the project's main legacy in the usability area that can be immediately taken up by project outsiders.

Web Tools

Privacy Dashboard

We developed the Privacy Dashboard, a Firefox extension. This tool combines several approaches to privacy preservation in the Browser. The Dashboard knows about all technologies that can be used and abused for user monitoring and tracking and it can block such monitoring. This includes Flash-cookies and client side DOM storage and all the other new client side mechanisms introduced by the new HTML5 Specification and already in use on the Web. Furthermore, the Dashboard implements a data track. This tool is inspired by the core of the "data self-determination paradigm". It records which information was given to which web site and stores it into a client-side SQL database. It tries to make such data accessible to users by some predefined queries. Further work will allow to a more efficient exploration of the data collected to track the trackers. The Dashboard also radically changes the paradigm of user interaction on privacy settings. In the past, users were often invited to set their preferences up front. This was very complex and over 90% of the users remained with the default settings as delivered with the Browser. The Dashboard makes the assumption that Privacy is dependent on the context and that knowing all contexts in advance is simply not possible. So the Dashboard doesn't set user preferences in advance, but learns them over time as the user browses the Web. A toolbar is asking about the user's preferences in the concrete context. Once a decision made, the Dashboard remembers that setting for future sessions. Over time, there will be less and less new sites and the user is bothered less and less while still having preferences that are as close to his needs as it can get. As an opt-in feature, the extension offers that data about tracking behavior of web sites can be shared in anonymized form to build a map of the tracking parties on the Internet. For the future success of the Privacy Dashboard, we have made it available as open source hosted by W3C.⁸ The extension is available on the Mozilla web site for download.⁹

⁸ <http://code.w3.org/privacy-dashboard>, <http://www.w3.org/services/privacy-dashboard/>

⁹ <https://addons.mozilla.org/en-US/firefox/addon/privacy-dashboard/>

Dudle – Collaborative Group Establishment

An often-used application, delivered through the Cloud model, is the one of collaborative group establishment. Based on an analysis of scenarios and the different group building stages, the project has developed theory and a tool for privacy-enhanced collaborative group establishment.¹⁰ The tool can be used such that privacy can be traded off against decision supporting information being available for group establishment, thereby covering the continuum from the one extreme of all input schedule information of participants being revealed to the participants, meeting organizer, and hosting platform, to the other extreme of almost no information being available to the participants, organizer, and hosting platform, but decisions being performed by a cryptographic majority vote protocol. The tool is web-based and has been made available as open source.

Life-long Privacy

A main goal of PrimeLife was to investigate privacy for life, that is, life-long, sustainable privacy for users. Basically, sustainability is a multi-dimensional problem which requires a multi-faceted approach to be addressed. A main outcome of the project as a whole is that we have discovered mechanisms and built prototypes for the protection of privacy throughout our lives. The goal of life-long privacy is not achieved by a single technology or system, but a set of technologies in different areas, each protecting privacy for a specific part of users' online interactions. The development and deployment of such a set of technologies is one major step forward for the protection of user privacy in a sustainable manner.

Sustaining privacy requires a combination of data minimization and policy-driven enforcement of data that needs to be released, together with mechanisms that allow a user to assess trustworthiness of service providers, easy-to-use interfaces and icons, cryptographic protocols etc. Many of the individual aspects of sustainability of privacy have been investigated in the project, also with prototypes being built. Such a broad approach of tackling all mainstream classes of use cases is a prerequisite for sustainable privacy.

We have specifically elaborated on life-long privacy from a legal perspective and put together requirements to act as basis for our dedicated prototype in this area. Thereby we found delegation to be a key feature necessary for life-long privacy and identity management.

As a specific applied part of the work on life-long privacy we investigated a scenario, namely life-time personal data management by the example of a backup prototype. A prototype was built showing the feasibility of our ideas for this scenario. The prototype allows a user to reflect their different areas of life, such as work and personal, by tagging her locally-stored data. For data of an area of life, a user can then specify policies on how and by whom a backup of such data should be recoverable, with delegation being a main concept. Access to data is granted on a policy basis, with data being securely held in cloud storage services. This allows for giving the right persons access to parts of the data on an as needed basis throughout the user's life.

Economic Considerations

The main results in the economic area of our work comprise a methodology for an economic valuation of IdM assets and capabilities of organizations and an assessment of the untapped potential in terms of identity management of those. It has been studied how such assets and capabilities can be leveraged to turn the organization into an identity service provider and thereby creating additional value from the exploitation of those unused resources. Furthermore, concrete such assets and capabilities were identified and analyzed and scenarios for value-added identity management services were discussed. (D6.1.2)

Our economic results on IdM enablers can help organizations generate additional value by leveraging already-available assets and capabilities for identity management purposes. Such additional value generation from so far unused assets may be an important driver for bringing more advanced identity management protocols into practice and thus additional value not only to the organization, but also users and service providers that benefit from such new IdM offerings. Think of mobile operators or other institutions with strong identity verification processes during

¹⁰ <http://www.primelife.eu/results/opensource/63-dudle>, <https://dudle.inf.tu-dresden.de/?css=css/PrimeLife.css>

customer registration that may be able to leverage their customer identities to offer their users secure (and privacy-preserving) identity management services.

Another result related to economic aspects comprises the understanding of adoption of identity management in different scenarios and for different identity management architectures. This includes results on identifying obstacles and opportunities for IdM infrastructure deployments as well as the technical part of the work of integrating available web-based standard protocols into an overarching IdM infrastructure to overcome some of the known obstacles.

Summary

As shown in this section, PrimeLife has substantially advanced the space of foundational research and practical applications of the results in multiple areas of privacy-preserving identity management. We have addressed problems and found solutions at various levels, starting from the infrastructure up to the applications. A particular strength of our research approach was its interdisciplinarity including technical, social, legal, and economic considerations. The project has executed a concerted approach of creating theory results, turning those into practical applications, open sourcing key prototypes, and bringing the technologies to standardization to drive future adoption. We have produced technology that helps users sustain their privacy throughout their lives. A particular part of this is technology that allows for user-centric and dynamically-configurable control over personal data in interactions that involve personal data which is one cornerstone of life-long privacy. Multilateral settings such as complex service compositions or social interactions are covered by our approach. Another cornerstone for life-long privacy is to not release personal data at all, that is, to employ technology for realizing data minimization.

Potential Impact, Main Dissemination Activities and Exploitation

PrimeLife has created results during its 40 months of project runtime that have already influenced the technology landscape and have potential for further impact in the mid-term to long-term future. We next give an overview of where we expect potential impact in the technology, social, and economic areas and in which areas we have already created traction during our project runtime.

Historically, PRIME, the predecessor project of PrimeLife, has set a landmark in European privacy research and created traction in technology, policy making, and society at large and made privacy a more discussed topic of interest. PrimeLife was targeted at continuing this successful venture of changing the European landscape, but with a broader focus than data minimization which was PRIME's main focus. PrimeLife has, in addition to continuing PRIME's successful work, targeted classes of applications that, during the PrimeLife project, have emerged to be the true game changers in the Internet at large as potential candidates for enhancing their privacy due to the particular privacy threat they create. As another major goal, PrimeLife has set out to investigate aspects of sustainable, life-long privacy and thereby created traction in a so-far not well-addressed area. In addition to its technical merits, our technologies and research in general will help create trust in the European information society and allow breaking down the barrier of slow adoption of certain electronic interactions due to a lack of trust.

In this section we summarize the impact PrimeLife has had so far and we expect in the future in the technological and socioeconomic arena. This is put in context with our main dissemination and exploitation activities we have performed. Thereby, we start at the concrete level of individual technologies and results of PrimeLife and carry this over to the larger impact the project will have in the European socioeconomic context in the mid to long term.

A Technology-based Perspective

We start with a discussion of impact in the technology area, thereby addressing the technologies mentioned in the preceding section on our main technical results.

The Social and User-driven Internet

Online Content Privacy

Our theoretical work, prototypes, and user studies in the area of privacy for user-generated online content has added privacy-enhanced functions to widely-deployed tools, e.g., MediaWiki or phpBB. Our *privacy-preserving reputation and incentive schemes* for Wikis as well as our privacy-preserving access control scheme and awareness extension for phpBB are built on the Identity Mixer anonymous credential system, thereby relying on this technology getting some deployment. Once this prerequisite is fulfilled, those tools allow for major improvements of information quality and trust on the web, while preserving privacy of users and giving them more fine-granular control over who can access certain content they create. Content quality today is a major issue and hinders the full potential of user-generated content, which is one of the key sources of knowledge in the information society, to be unleashed.

Social Network Privacy

With our *Clique* prototype and the related theoretical research, e.g., on *audience segregation*, we have demonstrated that better control of personal data in social networks than is offered by today's systems is practically feasible. We gained substantial media attention in newspapers and radio for our work and have the system deployed with multiple hundred of real users. We have shown how the functionality can, to a large extent, be built on top of the premier open source social network Elgg. The substantial media coverage also led to discussions on social network privacy with an important Internet stakeholder in the Netherlands and an invitation to talk about this topic at a Dutch high school with multiple hundred pupils, thus creating potential multipliers for our ideas and creating further discussions. Our results are available as open source and can be picked up by the maintainers of Clique or other social networks. The main impact of our research and development work, though, is that we have elaborated the concept of audience segregation and multiple other privacy concepts and showed that their realization in a practical system is feasible. The media attention helped convey the ideas to a large audience. In terms of further take-up of the ideas, we rely on social network providers to get interested in or users demanding such or similar technology. Properly implemented audience segregation technology will help users to easily define the audience for

their data items and to become aware of who may see which of their profile data which contributes substantially to proper life-long management of one's identity and preserving privacy.

PrimeLife's *Scramble!* technology provides a solution to the social network privacy problem from a different, orthogonal, angle: It allows users to define the audience of profile data independent of the social network provider and have the policy enforced through encryption. As it does not require the social network providers to play along, and only requires existing infrastructure, real-world deployments are to be seen soon. The tool has been made available to the open source community and plans exist for its future maintenance. The tool has been shown at conferences, including demos for further dissemination among the scientific audience. Scramble! offers users an orthogonal data protection mechanism to Clique. The high potential of Scramble! is due to its independence of service providers' support or new infrastructural requirements. This explains its substantial impact potential and probability of getting adopted by the community. In conjunction to Clique, our method for utilizing social networks to simplify key management in the Web of Trust can make the tool applicable to a wider audience.

PrimeLife's research work on the Like!-button of Facebook and how both members and non-members get tracked across Web sites they visit has gained major news coverage and already has had impact in the field. It has created awareness in the public on such tracking going being performed by this major social network platform. Also, Facebook adapted its software and multiple investigations by data protection authorities have been triggered. A substantial long-term impact is expected that social network providers like Facebook may make software deployments with stronger consideration of privacy of their offering.

Foundational Research

In addition to the results already mentioned above, further results were obtained in different areas that are crucial for privacy in different areas of life of people as well as for sustainable privacy throughout people's lives. Regarding basic research in the area of anonymous credential systems, we have progressed the state of the art substantially, particularly geared towards bringing the system towards better deployment. Thus, we have followed a closely-integrated strategy of theory development and its implementation in our open source library. The further cryptographic research has made major theoretical and practical contributions with different horizons of impacting future systems and making new ways of (commercial) electronic interactions possible. Those basic research results will have a mid-term to long-term opportunity of getting used in practice, but can then have major impact in terms of new value-added services that are not possible in that way today or for strong privacy properties, or a combination of both.

Data Minimizing Interactions

In this area, we have the main technical result of a stable implementation of *Identity Mixer*. The code is available as open source and well maintained and already now used by multiple research organizations in Europe and the USA, which we are aware of and interact with. Those use it mainly for (applied) research projects; e.g., a national eID card based on an anonymous credential system or Identity Mixer on smartphones. The results of our research realize the concept of data minimization to the extent possible through technology. The technology now being freely available to the public in a stable implementation and with stable API and usable for commercial applications, makes it an ideal candidate for having high impact in the midterm. The open source library is well maintained which helps increase its adoption by third parties.

The topic of data minimization and particularly the technology of anonymous credential systems has been gaining traction substantially over the last few years and has become an increasingly researched topic, also regarding infrastructures built around this base technology. We expect that the use of Identity Mixer will see further growth in research projects which will pave the way for future deployment of the technology due to increasing the understanding of the technology on a broader basis. We have also shown the feasibility of executing the Identity Mixer protocols on standard smart cards which is particularly important for high-assurance applications, such as e-government. Related to anonymous credential systems, the project ABC4TRUST¹¹ has been launched, in which both the Identity Mixer and the related U-Prove technologies are being further progressed towards being ready for production deployments. One goal of this project is to unify the technologies on the API level and build a common infrastructure around them. Further projects building on it are di.me¹² and FI-Ware¹³. Overall, we have grown the

¹¹ <http://abc4trust.eu>

¹² <http://dime-project.eu>

ecosystem around Identity Mixer substantially through our efforts in the PrimeLife project and we see high impact for the technology in practice in the coming years. Efforts in PRIME and PrimeLife on anonymous credential systems theory, architecture, and implementation have substantially contributed to the fact that this technology is being acknowledged broadly as being one important building block of future systems and that the research community and industry there is substantial traction in the field of anonymous credentials today, e.g., in the ABC4TRUST project that aims, as one of its goals, at a unification of the technologies at the interface level. Before PRIME and PrimeLife's efforts, the technology was not widely known and considered impractical by many. This shows the success of our long-term strategy behind the technology and its development from theory towards practical deployment.

The complement to Identity Mixer, the credential-based access control part of our policy engine, is another prerequisite for integrating Identity Mixer into practical deployments. We have meanwhile made the policy engine for credential-based access control available as open source which gives us the second key component for realizing data minimizing transactions in practice. We expect that the component will be adopted by the research community as another building block for data minimizing transactions and that it will help us in getting closer to real world deployments. The component will be used in the ABC4Trust and FI-ware projects.

Both the Identity Mixer library and the related policy component are being used as foundational technologies in a number of existing projects by project partners which creates immediate value for those projects without the need for building such technologies on their own. It will also help to harden the implementation and drive the whole Identity Mixer system towards practical deployments. We expect also that many future project will make use of these components.

Once Identity Mixer or similar credential technology will be deployed and credentials available on a large scale, this will have a major impact on society by allows for substantially safer Internet through service providers relying on certified data instead of claims while increasing the privacy of users through data minimization and allowing for anonymous yet accountable transactions. The societal benefit will be new and safer applications through verified data as well as new business opportunities for European identity service providers. It will help increasing trust on the Internet through technical means and thereby reduce fraud and increase consumer confidence in information technology at large.

Data handling Policies and Service Compositions

Practically, data minimization is a solution to many practical future scenarios, but by far not to all ones. Therefore, we have invested in generating technology that allows users to agree with data recipients on the data handling practices for their data and to enforce those practices at all data recipients in a service composition. Our approach is through an advanced model of data handling policies that is also operable in the context of service compositions. It represents the data handling part of the PrimeLife Policy Language. This addresses a large part of the class of interactions in which personal data needs to be processed, which will also be of significance in the future, besides data minimizing interactions. Our policy system can help ensure that data processing is happening according to policies, thereby addressing also the ever-increasing outsourcing of parts of service provisioning. Our framework for bringing data handling policies into service compositions can help communicate the ideas to decision makers.

We will make the policy language specification and implementation architecture available in the form of open specification to boost future adoption of the technology. Aligned with this step, we have shared the core ideas with standardization bodies and liaised with the key players world-wide in this area to set the foundation for future standardization and widespread adoption of the technology. Project partners have plans to further develop the policy language and implementation and use it in future projects to make it ready for production use.

Our data handling policy efforts help future services become more reliable and transparent in terms of enforcing agreed data handling constraints, even through service compositions. This will help increase trust in those service providers and may act, in conjunction with other technologies, as a driver for growth of the European digital single market at large as one major inhibitor is a lack of trust. We think that practical deployments of (subsets of) the technologies are expected in the midterm.

¹³ <http://fi-ware.morfeo-project.org>

Identity, Trust, and Privacy Management on Mobile Devices

Technology progress towards Trusted Execution Environments for mobile phones and pushing this to a standard were our key results in the area of trusted mobile devices. Specific future exploitation of our results are expected to happen in the SEPIA project and through the MobiCore secure operating system for smartphones which will allow users to run applications within strongly-separated security partitions, including secure input and output. Such future systems will act as major enablers for secure mobile interactions at large. Particularly, this technology roadmap will enable mobile phones to act as secure holders of digital identities, such as eIDs, which can be conveniently used from within the mobile device. Thus, this technology will play an important role as enabler for a plurality of different future use cases.

Access control

The scenario of data outsourcing by users to external services, e.g., Dropbox or Google Docs, is becoming increasingly important for collaboratively using data. For confidential material such outsourcing is not an acceptable solution without applying measures to hide the information from the outsourcing server. Commercial services offering encryption usually do not allow for sharing of the content. Our solution overcomes these shortcomings by employing a cryptographic enforcement of the access control policy through encryption combined with according key management and key derivation algorithms. Our open source code can be integrated with a multitude of existing online storage systems by interested developers and thus add the security functionality on top of insecure (and cheap) storage solutions. We have example integrations into a web browser and a file management application on the client side and it can be easily integrated with further tools due to our open system architecture. This access control technology for outsourced data has the potential to boost the adoption of cloud storage systems as one can combine the usually considerably lower cost of the cloud storage model with the strong security provided by our cryptographic access control approach, thereby benefitting both storage service providers as well as the European citizen. The complete transparency of the approach to the storage provider, no requirements on additional infrastructure, and the freely-available source code ease the adoption and increase the potential impact of the tool as a community-driven effort. Our approaches for protecting biometric data in the data processing infrastructures, again through cryptographic means, is seen as a prerequisite to deployments of biometric systems as it is unacceptable that service providers learn such data on a large scale.

Web Tools

Privacy Dashboard

The Privacy Dashboard is an open source product with no new requirements on the available infrastructure. We have had a number of downloads of the Dashboard in an earlier stage of its history and moved it to the Mozilla add-on download site recently. We expect further development to take place on W3C's code hosting site¹⁴, such as new features, localizations, and community-driven documentation. Exactly the lack of requirements to new infrastructure or services makes the Dashboard a strong candidate for larger deployments within the short term as it provides immediate privacy benefit through better awareness and the possibility of making settings and blocking tracking to its users. The high potential of this tool is due to a large extent to it not making any additional requirements to infrastructure than what is there on the web as well as the immediate privacy benefit. As we track the tracking parties through a community effort, this may lead to stronger insight into the structure how users are tracked and in the long term also to changes in tracking behavior if the tool, or similar tools, get widely adopted.

Privacy-preserving Polls

Our deployment of the Duddle tool is frequently used for polls by external users. The tool allows users to perform polls while giving out substantially less personal data about one's (non-)availabilities than with other offerings. Exactly this makes the tool a specialized tool for minimizing data release for one specific, but increasingly-used, purpose. It is therefore one piece of technology for achieving a broad coverage of different areas of life while at the

¹⁴ <http://code.w3.org/privacy-dashboard>

same time, due to data minimization, is important for realizing key concepts of life-long privacy in this specific application area.

We are running our own server that is open to the public. The software has also been made available as open source on freshmeat¹⁵ and alternativeTo¹⁶ under a generous open source license. As of time of writing this report, we were aware of 6 deployments of the server by the community which clearly shows the acceptance of this tool by the open source community. The open source code base furthermore provides a good basis for its future development by the community and thus an even broader impact in the years to come.

Identity Management Enablers

Our work on the enabler concept for identity management can act as guidelines for organizations who may have identity management assets and capabilities to leverage those by becoming an identity service provider. Such exploitation of available resources of companies for secondary use for identity management may be an important factor in bootstrapping the future identity management infrastructures as it reuses already-performed identity verification and can be of lower cost than dedicated service providers. Of particular importance for our work in this area is that it is based on economic considerations and helps the organizations create additional revenue by exploiting their available resources. This may be able to provide, at least a partial, answer to the question of how to make advanced identity management economically viable. As we provide a process model, this can be directly applied by organizations.

Dissemination Results

We next outline our key dissemination results of PrimeLife – dissemination played a key role in making privacy live and has been executed in a concerted approach with the technology development.

Scientific Publications

As outlined previously, we have made major progress in research on PETs and disseminated many of our results on relevant, mainly international, conferences and workshops. This considerably contributed to pushing the technical knowledge generated in the project to the relevant community such that others can build upon our results. We thereby made major contributions to the technology foundation of the future which the international research community is building upon.

Open Source

Generally, our open source strategy has had impact in the field already within the project runtime as has been discussed further above. Much of our source code has been made open under licenses that also allow for commercial use of our offerings. We have focused our dedicated open source development resources on a handful of products to maximize their adoption and make them sustain. The user-targeted offerings can create value directly for end users. Our offerings allow other projects in both academia and industry to leverage our technologies free of charge and thereby accelerate technology adoption through research and new offerings. A privacy-related value add can be achieved with little investment and in relatively short time such that adopting projects can focus their efforts on the main features of the product or service being created. Thus, our open source strategy has substantial potential for influencing the field from a technology perspective in the future. Open source has potential of contributing in general to the creation of the European Digital Single Market. Using our open source infrastructure components means following the paradigm of privacy by design in the product to be created. Privacy by design is widely acknowledged as one foundation for realizing privacy in future information systems. Links to our open source

¹⁵ <http://freshmeat.net/projects/dudle>

¹⁶ <http://alternativeto.net/software/dudle/>

results are given in this document, a summary of our open source results and impact can also be found in D3.3.2. The open source section on our website hosts or points to all our open source offerings.¹⁷

Standardization

PrimeLife's strategy for standardization comprised a focus on few areas and making major contributions in those to bring privacy further towards practice. We have had major involvement in standardization activities, e.g., by being (co-)editors of standards. Most of our standardization efforts were closely related to our technical work, thereby leveraging the experience gained in the (technical) project work for the standards in a very-well concerted approach. The activities with standards bodies create privacy awareness with key people and can act as a major vehicle for adoption of our technologies in practice.

With a series of Workshops organised in cooperation with W3C, PrimeLife was able to have a major influence on the global agenda of Internet Privacy discussions. The seven Workshops triggered further standardisation in two cases and brought all major stakeholders to the table including high level involvement of the US Federal Trade Commission, the US Department of Commerce and the European Commission. PrimeLife was recognized as a game changing project that brought new technology options to the global table as it was able to demonstrate the practical relevance of its contributions and also acted as a convener for others to join in on the discussion. (See the separate Workshop reports for details.)

PrimeLife has been driving a standard regarding a privacy and identity management framework in ISO which brings much of our experiences in the technical areas from PRIME and PrimeLife towards an international standard. This standard will create a common ground for terminology as well as provide guidelines for using privacy and identity management technologies and thereby will communicate main ideas of our projects towards practitioners. The standard on the privacy framework particularly defines the new protection goals of transparency, unlinkability, and intervenability with the goals of covering privacy aspects. Our ISO results pave the way for an international convergence of views and terminology in the area of privacy and identity management with the goal of mid-term to long-term impact in practice, which is typical for such international standards.

Standardization efforts in PrimeLife have widened their scope. At the beginning, we mainly target the International Standardization Organisation (ISO), the UN-Internet Governance Forum (IGF) and the World Wide Web Consortium (W3C). During the project's lifetime we were participating and actively driving the PRIMCluster group, a group of other EU IST FP7 projects with similar standardization targets. Furthermore, the decision for XACML as the main target language of the project put a new and strong focus on the cooperation with OASIS that was already successfully started.

In addition to the ISO efforts, we were particularly active in more short-term and industry-oriented standardization activities. Of particular mention are multiple workshops we (co-)organized in the area of policy standardization that were targeted at bringing our technical results in this area to a relevant international audience. PrimeLife was instrumental for the discussions in this area and brought together the major industry players in the field to lay out the plans for the future of privacy policy languages.

Another major area of PrimeLife's standardization efforts is secure mobile platforms where we made major contributions to an API specification for Trusted Execution Environments (TEEs) at the Global Platform Alliance based on technical work done on our secure mobile phone prototype. This work can lead to a faster proliferation of mobile devices with hardened security for certain parts of their operation such that secure key storage, computation, and input and output can be provided to the user. Such a standard is an important step in the roadmap for large-scale deployments of secure mobile devices which opens the mobile space for use cases that have not been possible before for reasons of missing security. As one of the next steps, eID cards or other identities could be embedded into a TEE of a smartphone and thus make the phone a secure wallet for the user's credentials. Ultimately, one may see the combination of Identity Mixer as the most privacy-friendly electronic authentication scheme to date and such TEEs, thereby reaching one milestone of data minimizing interactions. It is planned, that the technology being developed is further exploited in the SEPIA project and in conjunction with the upcoming MobiCore technology of secure operating systems.

A summary of key PrimeLife actions related to standards as well as discussion about impact can be found in D3.4.3, a survey on relevant standards for privacy and identity management in D3.4.2/H3.3.2.

¹⁷ <http://www.primelife.eu/results/opensource>

Workshops, Collaborations, Summer Schools, Reference Group, and the PrimeLife Book

PrimeLife has had substantial involvement and leadership role in workshops world wide to reach out to different target audiences as a main part of our communication strategy. In the standardization area, we were instrumental in bringing together and holding discussions with the main players in the policy area. The discussions are ongoing and standards are about to be submitted related to this. This will help make future deployments of some of our technologies possible on a larger scale. The following consortia of projects have stated their interest in a cooperation or have subsequently participated in some kind of joint activity with PrimeLife: ABC4Trust, AVANTSAR, Daidalos, Daidalos II, DESIRE, di.me, Effectsplus, EnCoRe, ENDORSE, ETICA, FIDIS, GeoPKDD, Liberate, MOBIO, NESSOS, PEACE, PEGASO, PETweb, PETwebII, PICOS, PrivacyOS, SEMIRAMIS, SEPIA, SeVeCom, SMILE; TURBINE and VESUV.

We have also held two PrimeLife Summer Schools with an audience mix that was extremely interesting for our dissemination strategy: research students, people related to policy making, and industry staff. Main goals of the summer schools were to disseminate key concepts of the paradigm of privacy by design to audiences who can act as multipliers and carry the ideas further into academia, industry, and society at large.

Another set of our workshops was a series of targeted dissemination workshops focusing on specific topics each. An example is the federated social network privacy workshop that has been held in Berlin that brought together a large community interested in progressing privacy-enhanced social networks. Those events have the goal to instrument the discussions between relevant stakeholders as well as communicating our privacy-protection technologies and bringing them closer to people deciding on their potential use in the future.

Another component of our interaction strategy with the community was the execution of a series of meetings with the PrimeLife Reference Group comprising international experts. We solicited feedback from this group on our activities to get an external and neutral assessment of our work and do adaptations based on this feedback if perceived necessary,

Finally, the project has published a book that summarizes its research results.¹⁸ And of course, numerous research papers were published in scientific journals and conference proceedings and PrimeLife was advertised in a large number of keynote speeches. A selected set of research publications can be found on our project website,¹⁹ along with a selection of presentation materials.²⁰

Sustaining PrimeLife's results

PrimeLife had as one key goal to make its results sustainable in multiple ways to maximize the value we bring to the community and society. Our research results build a solid foundation for future work of the community at large to build upon. We have solved major research problems, some of them theoretical, many of them with immediate practical application. Through our prototypes we implemented, we did not only show the practical feasibility of our results, but also gave many of the prototypes to the people in the form of open source. As some of our products have already been adopted, we are confident that we have sustained impact in those areas and bring better privacy to the people. Another key factor for sustainability of results is their standardization with relevant bodies. Details of the individual areas of where we have invested to make our results sustainable are presented further above. We are sure that our approach of using a mix of different dissemination channels as outlined has had major influence in the field of privacy and identity management already and will have more impact in the future.

A Socio-economic View

We have so far discussed the impact of our work and results from a technology-driven view which we complement with a general view on the socioeconomic impact of our work in the future. We have executed a concerted strategy

¹⁸ Jan Camenisch, Kai Rannenberg, Simone Fischer-Hübner (eds.): "Privacy and Identity Management for Life", Springer Verlag, 2011.

¹⁹ <http://www.primelife.eu/results/articles>

²⁰ <http://www.primelife.eu/results/talks>

of technology development with an interdisciplinary team, open source, standardization, and dissemination to targeted audience groups. This approach has helped us create strong traction and could reach out to many stakeholders in the fields of privacy and identity management.

We have been able to solve the main goals set of for PrimeLife, namely creating solutions for the privacy issues emerging from the new interaction paradigms on the Internet, such as social networks, addressing the life-long privacy issue, and thereby building on PRIME technology as one of our foundations. Related to new interaction paradigms, our results have resulted in a major media interest and coverage due to essentially every Internet user being concerned those days. Our work on Facebook's user tracking practices has shown already major reactions, not only across Europe. The results have potential of major future impact, particularly also through the concepts we have elaborated and the discussions we have triggered.

In the field of life-long privacy, a field not well-researched so far, we have achieved conceptual results that may trigger further work in the area and act as foundation for future research. We have shown the feasibility of implementing certain facets of life-long privacy with our related prototype, based on once concrete scenario. From a technology standpoint, the overall project results contribute to a technical realization in two different ways: First, our results cover a broad area of interactions between users in today's Internet and thereby cover multiple areas of life in terms of electronic interactions. Second, our major results in data minimizing technology provides the society with the technology foundation to realize a key aspect of life-time privacy: Data scarceness. This means releasing only data that are necessary for the service to be provided, and nothing more, because the safest way of ensuring privacy is by not releasing data at all.

Our technology is, considering its current adoption process and future adoption potential, capable of making information technology more trustworthy and thereby increasing consumer confidence in ICT at large. In addition, the trustworthiness of technology can be communicated by technical means to the users. This increase in trust may directly lead to a more rapid adoption of information technologies because a lack of trust has been one of the main barriers in IT adoption. Widespread adoption of our technology and related growth of the digital economy will, in conjunction with interoperability measures, help create the European Digital Single Market which is considered a key driver for the Europe being able to sustain its standard of living.

Some of our privacy technologies are enabling technologies for ensuring freedom of speech online which can be directly related to core European constitutional values we help preserve in an online world with a recent trend of increasingly eroding privacy protection and services that aggressively obtain and process personal data in non-transparent ways.

A Guide to PrimeLife's Legacy

The following text that is available also on the PrimeLife Web site provides a short summary of PrimeLife's legacy and links to the key project results.

<http://www.primelife.eu/results>

A Guide to PrimeLife's Legacy

PrimeLife produced a wide variety of results, ranging from basic research to educational materials to demonstrators and product-level source code. All these results are available from PrimeLife's website. In an attempt to make our results more accessible, we here summarize the main results, grouped by the different PrimeLife Activities.

I. Privacy for Life – New Concepts for Privacy

The aim of Activity 1 was to understand the various facets of privacy and identity management for scenarios and requirements that arise from Web 2.0 applications such as social networks, on the one hand, and the management of personal data throughout one's life, on the other hand.

Web 2.0 Applications

PrimeLife has identified two main issues: The first one is how users can detect and determine who has access to the data they make available, i.e., how they can segregate their audiences, and the second one is how users can assess the trustworthiness of information provided by others.

PrimeLife has come up with a number of solutions that enable audience segregation ([D1.2.1](#)). First, we have implemented our own social network platform [Clique](#) that enables users to easily set the audience of their postings and profile attributes. For the cases where the platform operator is not trusted, PrimeLife has developed a Firefox plug-in called [Scramble!](#) that achieves audience segregation using encryption. Second, we have integrated privacy-enhanced access control for collaborative workspaces based on [Mediawiki](#) and [phpBB](#).

Addressing the second issue, the focus has been on developing new and advancing existing mechanisms such as user reputation and certification, trust-related metadata, privacy-friendly incentive system, and trust policies. These mechanisms have undergone a conscientious validation process by employing them in selected demonstrators, which are a trustworthy [message board](#) and the [MediaWiki](#) system that has been enhanced with author reputations, and user experiments.

Sustainable privacy and identity management throughout one's whole life

In the light of the world-wide unsolved challenges for privacy throughout life, PrimeLife has elaborated requirements and methods to tackle this problem space. It has turned out, that one of the key problems here is the management of one's personal data during the different areas and stages of life, delegation of rights and duties, and the dynamics of all of these. This includes, for instance, allowing a delegatee to access one's data in case one is in hospital and unable to act in such a way that access is denied to the delegatee if one is not in hospital. A detailed report and prototype are available ([D1.3.1](#) and [D1.3.2](#)).

II. Privacy-Enhancing Mechanisms

Activity 2 was concerned with the investigation of open privacy issues and researching novel solutions and mechanisms that can be exploited as building blocks of future privacy-enabled technologies and applications. Besides the description of our research results that appeared in top international journals and conferences, PrimeLife's work also resulted in several prototype tools realizing the novel technologies developed by the activity so to make them usable by other activities within PrimeLife and by external parties (via the open source PrimeLife activities). We highlight the main results below and refer to the annual research reports for all results and details and references to our scientific publications ([D2.1.1](#), [D2.3.1](#), [D2.4.1](#)).

Cryptographic mechanisms

PrimeLife has developed a number of novel cryptographic schemes, mechanisms, and protocols (e.g., anonymous credentials, delegation of such, searchable encryption, and oblivious service access) that support users in protecting their personal privacy. Also, a Java-based implementation of the [Identity Mixer \(“idemix”\)](#) anonymous credential system that allows users to authenticate anonymously has been maintained and extended by the project.

Mechanisms supporting users' privacy and trust

The project has also developed novel mechanisms granting users the ability to control their privacy (e.g., transparency support tools) and, at the same time, to support interaction and collaboration of group/community members (e.g., privacy-respecting establishment of collaborative groups, and trust management via interoperable reputation systems). One tool that is available is [Dudle](#), a privacy-enhanced scheduling application.

Privacy of data

PrimeLife investigated novel metrics and techniques supporting the management of privacy requirements as well as of efficient accesses to large data collections (e.g., shuffle index). One result of this is [Pri-views](#), a Java-based tool that, given a collection of data, a set of sensitive associations, and a set of visibility requirements, computes data views in a way that no confidential information is released and required visibility over the data is satisfied.

Access control for the protection of user-generated data

A number of novel techniques for enabling the enforcement of access restrictions on user-generated data disseminated by external servers were put forth by PrimeLife. These techniques resulted in the tool called [Over-encrypt](#), a client-server web application for the dissemination of encrypted resources, and the enforcement of an encryption policy efficiently implementing access authorizations on the encrypted resources.

III. Policy Languages, Authorization and Access Control

Policy languages are a key ingredient for the deployment of data minimization technologies such as [Identity Mixer](#) and the protection of personal data. PrimeLife spent a considerable effort and obtained strong results in the space of policy languages. First, we collected an extensive list of requirements within and outside of our project. We then performed scientific research to address the technical challenges posed by these requirements. Our results have appeared in major conferences and journals in the field, and cover areas as diverse as policy matching and composition, credential-based access control, sensitivity metrics, and the relation between technical and legal policies. Finally, we carried a number of our research findings into the design of the PrimeLife Policy Language (PPL), which offers a holistic approach to privacy-enhanced access control and data handling. We demonstrated the viability of our approach in a prototype implementation of the PPL engine. The credential-based access control component of PPL was released as open-source software, acting as a policy front-end to a variety of technologies, in particular Identity Mixer credentials. The following documents summarize this work:

- Extensive requirements document ([D5.1.1](#))
- PrimeLife Policy Language (PPL) specification ([D5.3.4](#))

Some of these concepts were input to standardization at [OASIS](#), in particular an attribute predicate profile for SAML and XACML.

Finally, PrimeLife has made [available an open-source credential-based authentication framework](#) that integrates with [Identity Mixer](#) but also works with other credential systems such as X.509 attribute certificates.

IV. Human Computer Interactions

The protection of privacy and managing identity requires the involvement of users and it is indeed crucial that they understand how their data is dealt with by whom in what way and that they can effectively manage their data. To this end, Activity 4 has developed novel HCI evaluation methods and has conducted research on mental models and metaphors for PETs. Besides, it has developed and tested user interfaces for credential

selection, policy authoring, a tool keeping track of the data users reveal, and all other open source products and prototypes developed within PrimeLife.

In doing this, PrimeLife has developed new methods, patterns, and guidelines that might be of interest:

- PET USES (Privacy-Enhancing Technologies Users Self Estimation Scale), which has meanwhile also been used by other projects
- HCI Patterns for PETS ([D4.1.3](#))
- Guidelines how to design and how to evaluate PETs ([D4.1.6](#))

V. Infrastructures and Privacy

Infrastructure aspects have a significant impact on the adoption, security and privacy functionality of IdM systems in general, and of privacy-enhancing IdM systems in particular. Nevertheless, they are often overlooked. To fill this gap, Activity 6 researched service infrastructures capable of dealing with user-provided personal data in a secure and legally compliant way. In particular, multi-layered, cross-domain service composition scenarios (e.g., SOA) and the implications of down-stream data usage in larger systems were investigated ([D.6.3.1](#), [D6.3.2](#), H6.3.3). Also, the advantages of secure mobile devices in such scenarios were studied ([D6.2.1](#), [D6.3.2](#), [D6.2.2](#)). The key results were validated by the implemented complex test scenario using the PPL engine and evaluated against technical and legal requirements ([D6.3.2](#), [D6.3.3](#)). In particular, the following documents are suited for use by other projects:

- A simple, structured, and transparent economic valuation method for privacy-enhancing identity management services ([D6.1.2](#))
- Standardized APIs for isolation and storage in Trusted Execution Environments ([D6.3.2](#))
- Technical and legal requirements for privacy in SOA ([H6.3.1](#))
- An “Abstract Privacy Policy Framework” as blueprint for using privacy policies in service infrastructures ([D6.3.2](#))

VI. Standardization, Education, and Open-Source

Raising awareness of the threats to privacy in a digital world and of the existence of mechanisms that allow for the protection of privacy was a main goal of PrimeLife. In particular because many of these mechanisms are counter intuitive and somewhat more difficult to use than the privacy-invasive alternatives.

Education

PrimeLife has organized a number of [summer schools](#) and tutorials and has published educational materials. The latter are available from the PrimeLife website. Also, the summer schools were very successful and a committee has been formed that will continue to organize these schools in the [coming years](#). A summary of PrimeLife is published as a book by Springer. In particular, Chapter 26 of that book gives a list of recommendations to industry and policy makers.

Open Source and Standardization

Most of the tools and demonstrators from PrimeLife are available for download and free use. Indeed, some of these tools have been or currently are being picked up by other EU-funded projects, including [ABC4Trust](#), [FI-WARE](#), [SEPIA](#), and [di.me](#). Those are just a few projects that employ results from the [PrimeLife project](#).

Also, participants from PrimeLife are involved in many standardization initiatives such as [W3C](#), [ISO](#), [IETF](#), and [OASIS](#) and provide input from the project.

Project Fact Sheet

Start date: 01 March 2008

Duration: 40 Months

Budget: ~15 Million €

EC Funding: 10,2 Million €

Funding Scheme: FP7-ICT integrated project

Consortium

The PrimeLife Consortium comprises partners from seven EU Member States, Switzerland, and the United States of America. Each partner's unique competence complements the PrimeLife Consortium's joint competence that makes it unique in tackling today's most exciting privacy and identity management challenges. The following organisations are members of the PrimeLife Consortium: IBM Research GmbH (Switzerland; project coordination and scientific and technical lead), Unabhängiges Landeszentrum für Datenschutz (Germany), Technische Universität Dresden (Germany), Karlstads Universitet (Sweden), Università degli Studi di Milano (Italy), Johann Wolfgang Goethe-Universität Frankfurt am Main (Germany), Stichting Katholieke Universiteit Brabant (the Netherlands), GEIE ERCIM (France), Katholieke Universiteit Leuven (Belgium), Università degli Studi di Bergamo (Italy), Giesecke & Devrient GmbH (Germany), Center for Usability Research & Engineering (Austria), Europäisches Microsoft Innovations Center GmbH (Germany), SAP AG (Germany), Brown University (United States of America).

Technical Leader

Dr. Jan Camenisch

IBM Research GmbH, Switzerland

Project Manager

Dieter M. Sommer

IBM Research GmbH, Switzerland

Contact

primelife@zurich.ibm.com



<http://www.primelife.eu/>

4.2 Use and dissemination of foreground

Section A (public)

Introduction

Within the plan for using and disseminating foreground, the partners reported on their activities on their research findings and knowledge generated within the project (foreground). The partners further stated their plans for exploiting the generated knowledge and by which means they might have taken up on the exploitation activities.

This consolidated plan for using and disseminating knowledge V3 provides a picture of the activities undertaken during the whole project duration. It updates the "Plan for using and disseminating knowledge V1" (D3.1.3) and "Plan for using and disseminating knowledge V2" (D3.1.5). Public information on PrimeLife's ongoing dissemination activities are provided with the corresponding heartbeats H3.1.1 PrimeLife dissemination report V1 (month 12), H3.1.2 PrimeLife dissemination report V2 (month 24), and H3.1.3 PrimeLife dissemination report V3 (month 36) and will also be published as part of the final project report "D7.1.10 Final publishable report". This chapter introduces PrimeLife's project objectives, target audiences and the dissemination strategy to reach the identified audiences. The project's website takes a central role in the dissemination activities. Publishable results are made available for download at <http://www.primelife.eu/>

PrimeLife project objectives

The overall objective of PrimeLife has been to help enable individuals to retain control over their personal information. The PrimeLife predecessor project PRIME had already identified several emerging challenges in the field of identity management and had provided first solutions by means of user-centric identity management systems. While these were sufficient in traditional server-client style transactions, PrimeLife addressed challenges to privacy and identity management induced by the fundamental changes to the internet as they occurred. These changes comprised inter alia the change to a more community-based focus with interactions between users happening through applications such as virtual communities and web 2.0 technologies. Individuals want to retain and protect their privacy and control over personal data irrespective of their activities. However, contributing to these collaborative internet services may cause a life-long trail of personal data.

PrimeLife has tackled these challenges by having worked towards the following goals:

- Providing and supporting privacy throughout our lives, taking into account new ways of interacting an emerging Internet application services;
- Advancing the state of the art in the area of mechanisms supporting privacy and identity management;
- Making privacy real, largely disseminating its results through collaborative and educational activities, standardisation and Open Source initiatives.

The PrimeLife consortium had set up an effective and efficient management that drove the project towards meeting these objectives. The partners formed six activities consisting of multi-disciplinary research teams, which focussed on the following specific objectives all aiming at making sustainable privacy, trust and identity management a reality as shown in Figure 1 below:

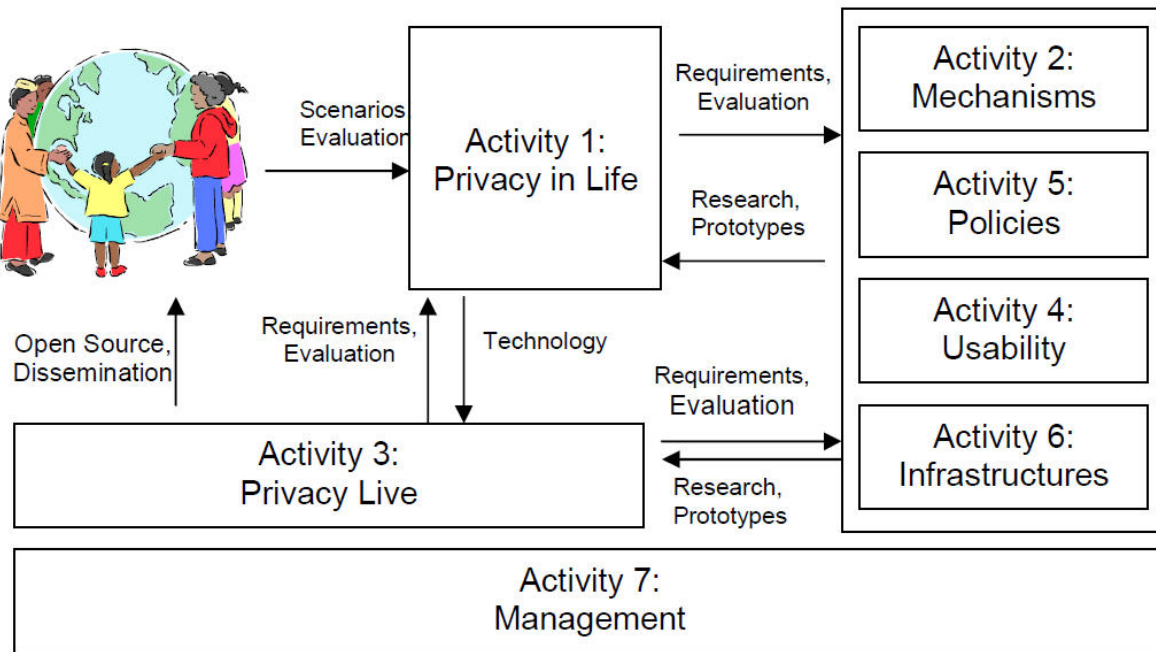


Figure 1: Interconnection of Activity 3 within PrimeLife

To reach the goal of providing and supporting **privacy throughout our lives** PrimeLife performed research addressing the following challenges:

- Sustaining privacy and identity management from birth to death.
- Providing user-centric and dynamically-configurable control over personal data in data-intensive interactions that characterise many of the virtual communities and collaborative applications.
- Adapt the PRIME concepts developed for privacy-enhancing identity management in bi- or trilateral settings to new multilateral technological and business settings.

Threats for the privacy of individuals could not be addressed with the knowledge and technology available before the project started. PrimeLife therefore performed various basic and applied technological research that was necessary to make privacy throughout life a reality. Important technology that PrimeLife covered are:

- **Tools:** The emerging Internet needs to be built on scalable and usable privacy technology components. Examples include privacy-enhancing cryptography, trust establishment mechanisms, as well as novel data protection and access control mechanisms for new types of user-contributed data.
- **Human-Computer Interaction:** Privacy will not be used unless it is usable. PrimeLife demonstrated how to make privacy technologies understandable and thus usable by larger groups of citizens.
- **Policies:** In order to provide configurable privacy spheres, it is important to build privacy policy support into the underlying mechanisms. These policies can then be used to configure technology to meet the regulatory, cultural, and individual requirements.
- **Infrastructure:** Many building blocks need privacy-aware infrastructure to function properly. We will show how to provide scalability and privacy.

Finally, the project aimed at capitalising on PrimeLife results and making them available on a large scale to other research projects as well as to the community at large. To this end, PrimeLife

- committed suitable results to **Open Source** initiatives,
- engaged in **standardisation bodies**, and
- provided **educational material and flyers**.

Reaching these objectives required extensive dissemination activities. PrimeLife pursued this goal by following its dissemination strategy as outline within the following section.

PrimeLife use and dissemination strategy

In accordance with PrimeLife's long-term goal of protecting privacy of individuals over their whole lifespan, dissemination of the project's findings took a central role. Reflecting its importance the consortium devoted Activity 3 "Privacy Live – Transferring results into practice" to this goal. PrimeLife put strong effort on dissemination activities based on this PR strategy identifying the target audiences. Activity 3 coordinated the dissemination of results, set up the public website and organised central outreach activities (like press releases, representation of PrimeLife at key events, organisation of public and closed workshops). In addition, and as one of the foundations of our outreach strategy, each partner is responsible and encouraged to publish individual results in-line with the project's work plan.

Activity 3 "Privacy Live" had a central role in the project dissemination activities and was well incorporated in the network of other activities. Activity 1 aimed at a life-long protection of privacy in the emerging collaborative internet. The activity researched and defined the requirements as an input for the research activities. Activities 2, 4, 5 and 6 built the actual privacy technologies. This includes basic research as well as applied research constructing privacy tools, privacy policies, and privacy-enabled infrastructures. Activity 3 aimed at the exploitation of the results. It provided the research findings for the real world. The activity transfers PrimeLife's research results into open source, standards, and actual products to enable privacy protection in upcoming product and service offerings. An overview of the information flow and the incorporation of the work packages on dissemination, of which Activity 3 consists, is given in Figure 2:

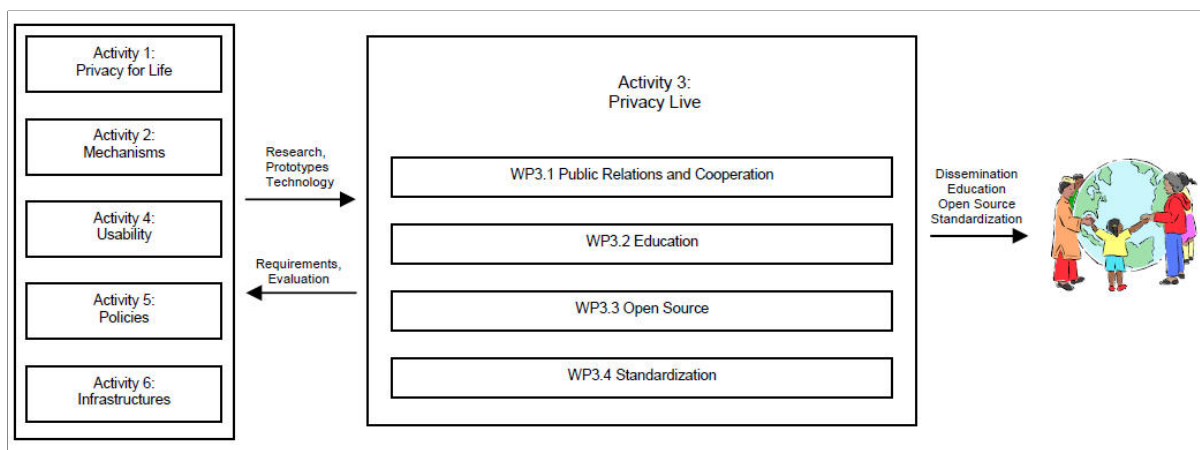


Figure 2: Activity 3 and dependencies

PrimeLife raises the privacy awareness of the general public and provides a platform for education on concrete ideas on privacy protection by means of organising summer schools, workshops a book publication and lectures. The book on the PrimeLife research results (D3.2.1) summarising the project's findings had consequently been scheduled for the end of the project (month 40). The book had been available for attendees of the PrimeLife Summit event in Lucerne, June 7th 2011. PrimeLife partners also engaged actively in educating students and the general public (see also section 0 below).

Exploitation directions

Research results have been and will be exploited, wherever possible, for creating value within all project partners' organisations. The following exploitation activities are pursued:

- *Open Source Software*: The consortium encouraged the use of research results including the developed prototypes as the basis for products, which are released via an Open Source licence. This aim had been reflected in a separate Work Package (WP3.3). For details, see section 0 below.
- *Commercialised products or services*: The industries partners may pick up project results to build on top own products or service offerings.
- *Think tank*: The PrimeLife partners made use of the project as a think tank on privacy and privacy technologies with a direct influence on their business (strategies, consensus building, standards, etc.).

- *Scientific publications:* In particular, partners from research and academia exploited the project's results via elaborating scientific publications.
- *Educational material:* PrimeLife supported the preparation of educational material and its use in teaching and raising awareness. Several academic partners and ULD used PrimeLife foreground for lectures at universities and schools.
- *Projects:* PrimeLife is expected to give rise to new research projects, and running projects may profit from PrimeLife's results in the area of privacy. PrimeLife kept close contact with several EC-funded and national projects. Research findings had been exchanged on conferences workshops and by personal contact between researchers.
- *Standardisation:* The project influenced standardisation initiatives. To this end, it reaches out to relevant communities as part of work package 3.4, and offered appropriate results for standardisation. (see section **Error! Reference source not found.** below).

The following key results are object of further exploitation. Please refer to section 0 below for further detail on the awaited results.

- Mechanisms
- Requirements
- Scenarios
- PrimeLife Demonstrators and Prototypes
- Assurance Methods
- Mock-Ups
- HCI Guidance
- Evaluation of PrimeLife Demonstrators and Prototypes
- Policies
- Infrastructure
- Dissemination Materials

Due to the variety of different partners the aimed use of PrimeLife's results varied, e.g. the industry partners pursued other goals than the academic partners, NGOs, or privacy protection authorities. A general overview of the exploitation plans is given by the table below. For further details on the individual partner's exploitation plans see section 0 below.

Exploitation plans		PrimeLife Partners							
		Industry					NGO, privacy commissioners		
		IBM	GD	EMIC	SAP		CURE	W3C	ULD
Results	Mechanisms	√			√				
	Requirements		√	√	√		√	√	√
	Scenarios								√
	PrimeLife Demonstrators and Prototypes	√	√						
	Assurance Methods						√		
	Mock-Ups						√		
	HCI Guidance	√					√		√
	Evaluation of Demonstrators	√	√				√		
	Policies	√		√	√			√	√
	Infrastructure	√	√	√	√				
	Dissemination Materials							√	√

planned exploitation
 possible exploitation
 Not applicable

Table 1: Exploitation by partners

Academic partners were intentionally omitted. The academic partners were disseminating the project's results to the relevant research communities by presentations at conferences and publications in relevant journals or books. Where appropriate the partners included research results in university lectures disseminating the findings to the next generation researchers and decision makers. However, PrimeLife partner TILT was also actively using interviews, mainly in Dutch radio or podcasts, as a powerful technology for disseminating key results to the young target audience.

Motivations and goals

When the predecessor project PRIME started in March 2004, the PRIME partners' motivation for extensive dissemination activities had been that many people had not been aware that their privacy was at stake in many situations and even if they had been, they had not been able to protect themselves. The lack of awareness has gradually changed. Due to several scandals concerning the loss and fraudulent exploitation of personal data in different European countries, the awareness for privacy-related issues was raised. Besides occurrences in the private sector such as inappropriate collection and transfer of data by employers or customer data by businesses, also incidents in the public sector and draft bills e.g. referring to data retention or the transfer of passenger name records in third states lead to extensive coverage of privacy related topics in the general press. Newspapers also reported about ways and possibilities to protect ones privacy and the need of identity management. However, deeper knowledge as well as effective, transparent, and easy-to-use tools for identity management was missing and the perception of privacy issues varied between member states and age groups.

Target audiences

The success of PrimeLife and beyond in the area of privacy and identity management primarily relied on the capacity of its participating experts to establish credibility, to interact and exchange information about the vision of PrimeLife, its approach, progress and results. In order to support the project's objectives, the identification of the key actors and the creation of a wider community of stakeholders were crucial. The following stakeholders had been identified and addressed while disseminating material:

- *Individuals*, who are end users and/or data subjects (so-called useses, i.e. persons about whom personal data are processed) of Information and Communication Technology (ICT) systems and applications. Users can for instance perform the roles of community members, employees, service subscribers, citizens, authors, customers, or clients within PrimeLife application areas. PrimeLife produced several software prototypes to be deployed by users. Users have been educated about the use of personal data and the deployment of PrimeLife applications. The usability of privacy tools is an important precondition for allowing users to utilise them. This issue had been addressed by Activity 4.
- *Media / Journalists*, especially those specialised in information and communication technology have been invited to spread information about the PrimeLife project and its results to the public and to special interest groups (e.g., readers of technical papers or relevant scientific journals). Contacts to journalists happened via interviews given by PrimeLife personnel and by invitations to workshops.
- *User and consumer associations* at national and European level like the European Consumer's Association (BEUC). Consumer association had been helpful in advertising privacy seals and other methods of privacy assurance, increasing both awareness and visibility concerning PETs in products. Contact had been established via the PrimeLife reference group and existing personal and institutional dissemination channels.
- *Education*, PrimeLife researchers disseminated results during lectures held and provided slides and informational material for specific topics to fellow lecturers.
- *Policy makers and parliamentarians*, nationally and at European level. They are representatives of the citizens as potential users and data subjects PrimeLife should protect their privacy interests and rights. They also have the possibility to promote PrimeLife-based solutions by for example creating legal rules for the obligatory deployment of privacy threat analyses, privacy audits and privacy-enhancing technologies and by facilitating this by budgetary allocation realising inter alia the public authorities to first hand purchase products, which have been awarded a privacy seal.
- *Privacy commissioners and Data Protection Authorities* in the EU member states and subsequently the Art. 29 Data Protection Working Party. They have been informed about PrimeLife could therefore promote the large deployment of PrimeLife-based solutions in governmental and in commercial organisations.
- *IT security organisations*, especially the European Network and Information Security Agency (ENISA), which aims at ensuring a high and effective level of network and information security within the European Union.
- *Research communities* (governmental and commercial) and other projects, e.g., in FP7, dealing with privacy issues and technology assessment organisations at national and European level have been stimulated to cooperate with PrimeLife partners in a scientific discussion and research on privacy-enhancing IdM.
- *Organisations that use information systems and process personal data*, like banks, insurance companies, credit card companies, toll collection companies, network operators, service providers, providers of central components for communities, advertisers, governmental authorities and providers of infrastructures. They perform the role of the data controllers (i.e. the entities that are responsible for the processing of personal data of users and useses), and as such they have to strictly follow data protection legislation. Privacy-enhancing IdM can assist such organisations in guaranteeing law compliance.
- *Standardisation organisations* at national and international level, like European Committee for Standardisation (CEN), World Wide Web Consortium (W3C), International Organisation for Standardisation (ISO), the Organisation for the Advancement of Structured Information Standards (OASIS) and the International Telecommunication Union (ITU), all working on identity management. Their cooperation was important for the transfer of PrimeLife results into standardisation and ensured interoperability with existing systems and concepts.
- *System developers, system designers, suppliers of ICT products and services* could be motivated to see PETs as a business enabler and therefore integrated PrimeLife concepts and solutions into their systems and products. As a result, they could help to trigger persuasive deployment of privacy-enhancing IdM solutions.
- *Business and industry associations, employer associations and trade unions* on a national and European level; their support was also needed for a broad deployment of PrimeLife-based solutions within organisations. They have been broadly informed about the opportunities that PrimeLife can provide both from a business and a user perspective.
- *Law enforcement authorities* at national level and international bodies like Eurojust, Europol and Interpol. Their representatives should participate in discussions with PrimeLife Partners and advise them about

legitimate law enforcement interests that have to be supported by PrimeLife-based solutions and that are in an appropriate balance with the privacy rights of users and uses. In particular, circumstances under which anonymity should be revoked in order to prosecute criminals have to be well defined and agreed upon.

A cross-section of these stakeholders were part of the PrimeLife Reference Group.

An overview of the audiences addressed by PrimeLife's past dissemination activities is given in Figure 3. Throughout the project, the consortium partners raised their engagement for dissemination towards all target audiences. Being a research project a natural focus had been set on disseminating knowledge towards the scientific community. Collaboration with other EC projects and conveying results towards industry and deployment were focal points during the second and third period.

When viewing Figure 3 below indicating which audiences have been addressed, please note that for each dissemination event multiple choices were possible as some of the dissemination activities reached several audiences. For example, the PrimeLife summer school primarily targets students, the academic community, and research personnel. However, dissemination to and discussion with other EC projects and stakeholders from the industry were essential part of the agenda as well.

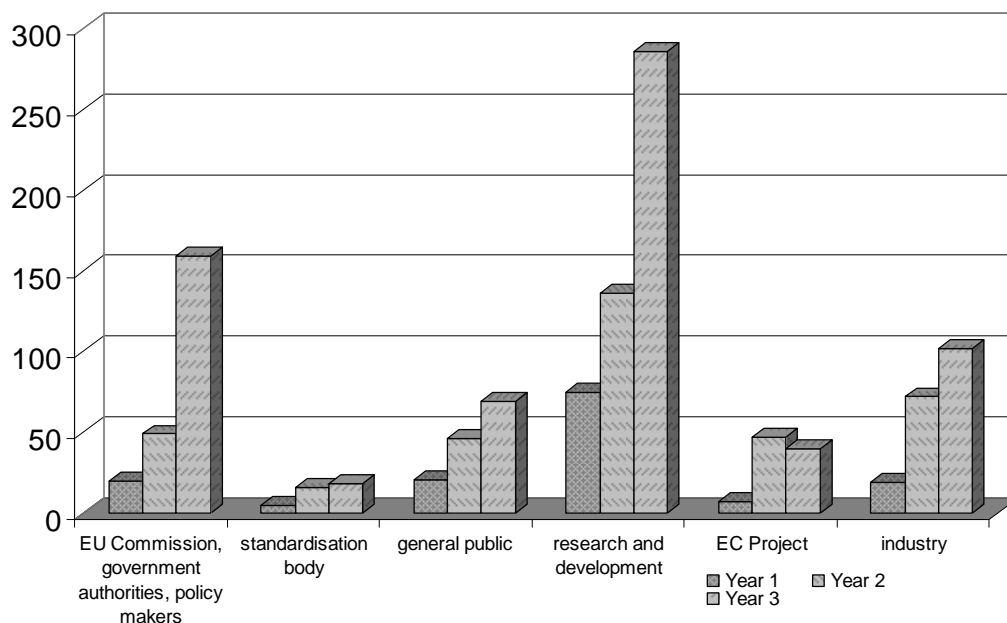


Figure 3: Types of audience addressed

Reaching the target audiences

During the project's lifetime, PrimeLife used standard dissemination channels for scientific results, such as articles in journals, papers at conferences and demonstrations at fairs. We made use of further ways to disseminate results, e.g., directly to users in communities or by providing Open Source software (see section 0). In recognition of the overall importance of the dissemination strategy, the consortium chose the approach considered the most effective by combining multiple media pathways, each selected for its suitability to the needs and resources of the particular target audiences concerned. Two major categories of dissemination channels were addressed: Permanent channels and PrimeLife-specific channels.

Permanent channels exist independently from the project and comprise

- Media
- Public events
- Technical publications
- Partners own channels

PrimeLife specific channels consist of

- PrimeLife's website
- Networking activities
- Summer Schools
- PrimeLife workshop series
- PrimeLife's internal website

The PrimeLife workshop series enabled the partners to disseminate results to a well-defined target group of interested experts in the specific section of PrimeLife's research activity.

To disseminate their results most effectively the partners have chosen the dissemination channels that fitted best to the target groups, which have been addressed by the partners in a long history of research networking.

Workshop series

Within the project's lifetime, PrimeLife has organised several different kinds of workshops:

- Workshops for the PrimeLife Reference Group that gave feedback on results achieved by PrimeLife results during the project's lifetime ("Reference Group Meetings");
- Summer Schools for researchers and students that taught about state-of-the-art and new results and trends on privacy-enhancing identity management;
- Standardisation Workshops that addressed standardisation initiatives;
- Workshops for journalists to explain PrimeLife's results and position the project in the identity management landscape;
- Cooperation Workshops for related projects, interested developers or other parties who discussed their own needs for PET modules and picked up PrimeLife's results to improve their own concepts and IT systems. Similar other projects (in particular potential follow-up projects) that could profit from the technical expertise gained within PrimeLife have been addressed.

Results Disseminated

The Plan for the use and dissemination of foreground contains two sections, hereafter called Part One and Part Two. While the "Plan for using and disseminating knowledge V2" (deliverable D3.1.6) is classified as an internal document some parts will be published as public heartbeat "PrimeLife dissemination report V3" (heartbeat H3.1.3). Part two will hold confidential parts of the dissemination report particularly some of the partners' individual exploitation plans. Part of the information will also be made available in D7.1.10 "Final publishable report".

Dissemination of Foreground

A major goal and focus of PrimeLife work was to make privacy "live". An entire activity (3) had been dedicated to transferring the project results into practice by making them widely available. In order to achieve this objective, PrimeLife presented solutions to protect and maintain one's private sphere and raised awareness concerning privacy and identity management in Web 2.0 applications, and throughout an individual's whole life.

In this chapter an overview on PrimeLife dissemination activities is given, thus refining the project's dissemination strategy it as has been introduced in section 0. The following section describes dissemination to the public, while the second section concentrates on the research community. The third section shows PrimeLife's outreach to standardisation bodies and initiatives and the fourth section deals with PrimeLife and open source. The fifth section gives an overview on different workshops that were held within the project's lifetime.

Dissemination to the public

One of the project objectives was to raise awareness for privacy and identity management issues and possible solutions. Therefore disseminating PrimeLife's results to the public was considered very important by all consortium members. The following table shows the selected dissemination efforts to the general public made during the project's lifetime. For detailed information, please refer to the table in Annex A. An aspect of the PrimeLife object to archive livelong privacy included the education and raising awareness for privacy with young persons. The second project year focussed on social networks and provided a good platform for addressing the public with basic privacy understanding, recent PrimeLife research results, and prototypes such as "Clique", "Scramble!" and "dudle". Several consortium members engaged in this work inter alia by visiting schools, giving interviews and taking up the topic in university lectures.

Table 2: Dissemination to the general public

Date	Dissemination Activity	Type of audience	Countries addressed	Partner involved
	Website			
Project start, May 2008	Project website	general public	All	ULD / W3C / all
	Press releases / Press coverage / Interviews			
Project start, 27 May 2008	Press release "European Union launches 16 Million Euro R&D Project on Privacy and Identity Management"	general public	All	ULD / all
March 2009	Interview with Marit Hansen: "Informationen bei Datenschutzvorfällen: Ja, bitte!", in: DANA 1/2009, Bonn, Germany	general public	Germany	ULD
16 March 2009	Interview with Marit Hansen, "Große Mehrheit sorgt sich um Privatsphäre im Netz"; press publication, Germany	general public	Germany	ULD
25 March 2009	Interview with Marit Hansen: "Großbritannien will soziale Netze überwachen", press publication	general public	Germany	ULD

Date	Dissemination Activity	Type of audience	Countries addressed	Partner involved
8 April 2009	Interview with Jan Schallaböck: "Demokratie und Datenschutz auf Facebook & Co", published at futurezone.orf.at	general public	German language area	ULD
8 May 2009	Interview with Marit Hansen: "Twitter: Private Daten auf dem Präsentierteller"; press publication	general public	Germany	ULD
23 May 2009	Interview with Marit Hansen: "Social Networks speichern gelöschte Fotos"; press publication	general public	Germany	ULD
25 May 2009	Interview with Marit Hansen: "Social Network Seiten – Hindernis beim Bewerbungsvorgang?"; press publication	general public	Germany	ULD
6 June 2009	Interview with Marit Hansen: "British Telecom – Rückzug aus Spion-Werbesystem"; press publication	general public	Germany	ULD
14 July 2009	Interview with Marit Hansen: "Datenschutz für Facebook-User unerwartet wichtig"; press publication	general public	Germany	ULD
16 July 2009	Interview with Marit Hansen; "Social-Network-Seiten sind wahre Fundgruben für Phisher"; press publication	general public	Germany	ULD
25 July 2009	Interview with Marit Hansen: "Europäische Bankdaten bleiben im Visier der US-Fahnder"; press publication	general public	Germany	ULD
14 August 2009	Interview with Marit Hansen; "Tatort Internet: Polizei will 2000 Cyber-Cops"; press publication	general public	Germany	ULD
October 2009	Interview with Marit Hansen: "Die Kriminalpolizei rät 3&4, Leitartikel"; press publication, pressto gmbh – agentur für medienkommunikation Published as "Anonymität ist verführerisch" in "Die Kriminalpolizei rät ...", pp. 22-28	general public	Germany	ULD
December 2009	Press coverage: PrimeLife was elected "Project of the month" by the NGO website Gov2u. http://www.gov2u.org/	general public	International	3rd party
20 January 2010	Press coverage on PrimeLife's Prototype "Clique" in Nederlands Dagblad, two articles, one on the front page	general public	Netherlands	TILT
30 January 2010	Interview with Bibi van den Berg on the release of PrimeLife's Social Network software Clique; press publication by Ernst-Jan Hamel: "Tilburg bouwt privacyvriendelijk sociaal netwerk"	general public	Netherlands	TILT
30 January 2010	Press coverage on PrimeLife Prototype "Clique" at Nu.nl	general public	Netherlands	TILT
1 February 2010	Radio coverage, Radio 1 interview on "Lunch!" about PrimeLife's prototype "Clique"	general public	Netherlands	TILT
18 February 2010	Interview with Marit Hansen on the service PleaseRobMe.com and general issues of online security and web 2.0	general public	Germany	ULD
26. February 2010	Interview with Marit Hansen on Social Networks for the Bayerische Rundfunk	general public	Germany	ULD
11 March 2010	Simone Fischer-Hübner: Radio Interview at SR.se, "Politikers identität karpas på nätet"	general public	Sweden	KAU

Date	Dissemination Activity	Type of audience	Countries addressed	Partner involved
10 June 2010	Simone Fischer-Hübner, Hans Hedbom: Interview in Forskning&Framsteg, "Integritetskris på nätet", 1 June 2010	general public	Sweden	KAU
2 January 2011	Peter Wolkerstorfer: "Ein Kondom für den Firefox", Interview published at http://fm4.orf.at/stories/1674864/	general public, radio coverage	Austria	CURE
	Flyers / Leaflets / Posters / Presentation Slides / Exhibition / Consultation			
March / April 2008	Participating in exhibition at The Future of Internet Conference, Bled, Slovenia	general public, other projects	All	IBM
June 2008	PrimeLife Presentation	general public	All	ULD, all
February 2009	Project flyer	general public	All	ULD, all
28 January 2009	Participating in symposium on Social Network Services organised by DPA of Rhineland-Palatinate and Second channel of German television broadcasting) on the occasion of the European Data Protection Day 2009	high school students	Germany	ULD
March 2009	Talks on privacy related topics at the CeBIT exhibition in Hanover, Germany	general public, IT specialists	Germany	ULD
3 April 2009	Jan Schallaböck: "A Netiquette for Social Networks", Joint presentation at Re-Publica 2009 and 2nd European Privacy Open Space (together with Ralf Bendrath, and Prof. Hendrik Speck) in Berlin	general public	Europe	ULD
23 September 2009	Kai Rannenber: "Privacy in a world of ambient and personalized ICT Services", talk at "The Net will not forget", European conference on ICT and Privacy, Copenhagen, Denmark	general public	Europe	GUF
15 September 2009	Marit Hansen: "Der gläserne Bürger", talk at Soroptimist Kiel, Kiel, Germany	general public	Germany	ULD
3 October 2009	Benjamin Kellermann: "Datenschutzfreundliche Terminplanung", presentation at the Datenspuren 2009, Dresden, Germany	general public	Germany	TUD
16 November 2009	Katalin Storf: "Datenschutz in Social Networks und Online Spielen", Mediatage Nord, Kiel, Germany	general public	Germany	ULD
20 November 2009	Identity Management; Kolloquium "15 Jahre kommerzielles Internet in Dresden", IBH IT-Service GmbH, Dresden, Germany	general public	Germany	TUD
30 December 2009	Benjamin Kellermann: "Privacy-Enhanced Event Scheduling", presentation at the 26C3, Berlin, Germany	general public	Europe	TUD
9 February 2010	Marit Hansen, Holger Brocks: presentations at Safer Internet Day 2010, Ahrensburg, Germany	general public	Germany	ULD
9 February 2010	Holger Brocks: "Datenschutz im Internet: Informationsabend" press coverage and presentation on the occasion of the Safer Internet Day 2010, Altenholz, Germany	high school students, parents	Germany	ULD

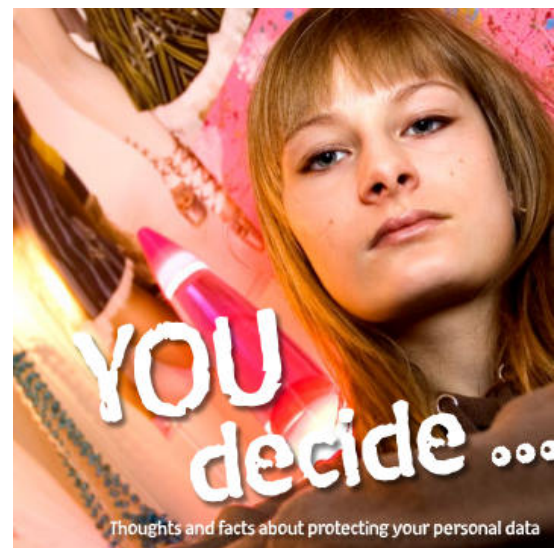
Date	Dissemination Activity	Type of audience	Countries addressed	Partner involved
3 March 2010	Harald Zwingelberg, Ulrich König: "Selbstbestimmter Datenschutz: Lösungen für mehr Transparenz in Webshops und E-Mail", presentation at CeBIT, Heiseforum, Hanover, Germany	R&D, industry, general public	Europe	ULD
23 March 2010	Chapters "8.2 PrimeLife – Identitätsmanagement im Fokus" and "2.3.2 Internationale Standardisierung", in: 32. Tätigkeitsbericht des ULD (2010), Landtagsdrucksache 17/210, https://www.datenschutzzentrum.de/material/tb/tb32/ .	policy makers, general public, governmental authorities	Germany	ULD
7 April 2010	Ronald Leenes: "Clique in 15 minutes"	general public	Europe	TILT
7 April 2010	Danah Boyd: "How Social Media is Reworking Privacy and Publicity"	general public	Europe	TILT
29 April 2010	Marit Hansen: participation in the panel discussion "Web 2.0: Dein öffentliches Privatleben", University of Applied Sciences, Kiel, Germany	general public	Germany	ULD
17 June 2010	Ronald Leenes: "Sociale netwerken die voldoen aan normen"	general public	Netherlands	TILT
21 June 2010	Sandra Steinbrecher: "Online Privacy and Identity Management", Salon im Kunsthof, Dresden	general public	Germany	TUD
30 August 2010	Marit Hansen: "Kontrollverluste durch Informationstechnik", presentation at Sommerakademie 2010 "Codex digitalis: Optimierter Persönlichkeitsschutz – digital und vernetzt", Kiel, Germany, https://www.datenschutzzentrum.de/sommerakademie/2010/	policy makers, general public, journalists	Germany	ULD
September 2010	Presentation of WP6.3 results at at EU ICT 2010 Brussels, Belgium	general public	Europe	EMIC, SAP, GD
16 October 2010	Benjamin Kellermann: "End-to-end-verifiable Voting am Beispiel von ThreeBallot und Scantegrity II", presented at Datenspuren 2010, invited talk	general public	Germany	TUD
19 February 2011	Booth presenting data protection and privacy for pupils at 1. Mini-Medien-Kompetenz Messe, February 19th, 2011, Kiel, audience: pupils, parents, teachers	general public	Germany	ULD
4 March 2011	Bibi van den Berg, Ulrich König: "Image is everything: Audience segregation in social network sites", presentation at the Heise booth, CeBIT 2011, Hanover, Germany	R&D, industry, general public	Europe	TILT, ULD
5 March 2011	Rigo Wenning, Ulrich König: "Tracking the trackers: Primelife Dashboard and dashbot", presentation at the Heise booth, CeBIT 2011, Hanover, Germany	R&D, industry, general public	Europe	W3C, ULD
6 March 2011	Ulrich König: "Privacy Icons in E-Mails", session slot on the privacy barcamp, Hanover, Germany	general public	Germany	ULD

Date	Dissemination Activity	Type of audience	Countries addressed	Partner involved
29 August 2011	ULD-Sommerakademie "Organisierte Verantwortung/slosigkeit", Kiel, Germany	policy makers, governmental authorities, general public	Germany	ULD
	Lectures / Teaching			
16 April 2009	Ronald Leenes: "Privacy & identity in sociale netwerken", Introductiecollege UvT, talking to students and parents	students, parents	Netherlands	TILT
12 October 2009	Isabelle Oomen, Lecture about privacy and social network sites at the University of Amsterdam for master students Philosophy	university students	Netherlands	TILT
November 2009	Slim Trablesi: "Security and Privacy Research", lecture at Ecole Nationale d'Ingenieurs de Tunis (ENIT)	university students	Tunisia	SAP
2 December 2009	Maren Raguse: "Identitätsmanagement Privacy4Life", lecture at University of Applied Science Kiel	university students	Germany	ULD
5 December 2009	Ulrich König, Harald Zwingelberg: Coaching for High School student's project on "Web 2.0 – social networks" at Berufliche Schule Wirtschaft Kiel. The students produced a 80 min. presentation including a film, a theatre play and a talk on the topic	high school students	Germany	ULD
15 December 2009	Magali Seguran: "Security and Privacy Research", lecture at Jean Moulin University Lyon	university students	France	SAP
2009	Kai Rannenber, Several Teaching Lessons at GUF on PrimeLife related topics	university students	Germany	GUF
14 January 2010	Harald Zwingelberg: "Identity Management in Social Networks", lecture at Wirtschaftsakademie Schleswig-Holstein, Kiel, Germany	university students	Germany	ULD
4 February 2010	Harald Zwingelberg: "Identity management and lifelong privacy", lecture at Wirtschaftsakademie Schleswig-Holstein, Kiel, Germany	university students	Germany	ULD
2010	Several Teaching Lessons at GUF	university students	Germany	GUF
12 May 2010	Marit Hansen: "Datenschutz und Technik III – Datenschutzfördernde Technik", lecture at University of Kiel, Germany	university students	Germany	ULD
2 June 2010	Kai Rannenber: "Privacy by Design – Auf dem Weg zu einem effizienteren Datenschutz" Reimers-Kolleg, Bad Homburg	university students	Germany	GUF
21 December 2010	Harald Zwingelberg: "Identitätsmanagement, lebenslanger Datenschutz", lecture on identity management and lifelong privacy, held at the University of Applied Science Kiel, Germany	university students	Germany	ULD

Date	Dissemination Activity	Type of audience	Countries addressed	Partner involved
17 February 2011	Harald Zwingelberg: "Schutzziele, Identitätsmanagement, lebenslanger Datenschutz", lecture on Privacy Protection Goals, IdM and lifelong privacy, held at Wirtschaftsakademie Kiel, Germany	university students	Germany	ULD
11 May 2011	Marit Hansen: "Datenschutz und Technik III – Datenschutzfördernde Technik", lecture at University of Kiel, Germany	university students	Germany	ULD

Teenage pupils and social networks

A specific target group PrimeLife had identified are pupils and students. Initially it had been intended to provide own teaching material for teenage pupils at primary schools in particular related to privacy issues related to social networks. Soon ULD figured that the European Parliamentary Technology Assessment (EPTA) has already launched a Norwegian based program "You Decide – A privacy campaign for primary schools" having produced a comprehensive brochure tailored to the age group. ULD took over a partnership to provide a German translation for this brochure with involvement of ULD's PrimeLife staff. Subsequently ULD held lectures at several primary schools in the region about privacy implications of social networks and how to act privacy aware protecting ones own and others private sphere. Slide sets provided for these lectures are available for download at: <https://www.datenschutzzentrum.de/schulvortrag/>. For more details about the brochure "You deice" as well as English and Norwegian download versions visit: <http://dubestemmer.no/en/> the German version is available at <https://www.datenschutzzentrum.de/download/entscheide-du.pdf>.



Alongside the engagement with educating the target group ULD staff Thilo Weichert, Marit Hansen had been jury members of contests for the school pupils. One had been for school magazines covering issues of privacy in social networks. The other contest is still open targets issues of digital oblivion. While also targeting researchers and the internet community there is a special price for the best submission by pupils.

In addition, PrimeLife consortium partner TILT targeted the group of the teenage pupils. In particular, during the second project period TILT presented the PrimeLife prototype "Clique" at several occasions in press interviews, and radio interviews. The live demo system available at <https://clique.primelife.eu/> of Clique raised high interest. Over the past year and a half close to 2000 users have subscribed to the system. At first, these were mainly Dutch speaking users, yet over time Clique has managed to reach a European audience, and now even has users from other parts of the globe as well. PrimeLife researchers from TILT also visited a high school to educate about privacy implications of social networks. Slide sets of the presentation they gave are available for interested persons and teachers.

Dissemination to research

PrimeLife, as a research project, addresses with many of its research work and deliverables the research community, also inviting readers to discussion. The importance of PrimeLife research becomes evident when studying the existing research report of Activity 2, referenced D2.2.1 (First report on mechanisms), the first period's research report of Activity 4, referenced D4.1.1 (HCI Research Report – Version 1), and D5.2.1 (First research report on research on next generation policies). This research was continued in Activity 2, D2.3.1 (Second report on mechanisms), the second period's research report of Activity 4, referred D4.1.3 (HCI Pattern Collection – Version 2) and within Activity 5 in D5.2.2 (Second report on research on next generation policies). The final research results had been available at the end of the third period as D2.4.1 (Final report on mechanisms), D4.1.5 (Final HCI research report), and D5.2.3 (Final research report on research on next generation policies).

During the lifetime of PrimeLife, demonstrators and prototypes were designed and implemented, to understand and address privacy users in emerging real life scenarios (see also section 0). Legal and technical requirements were elaborated to facilitate privacy-enhancing identity management solutions.

This prototyping was supported by research Work Packages that elaborate on mechanisms for the prototypes, general underlying research questions, and the infrastructure perspective such that they meet the requirements from a legal, social, economic, and application point of view.

PrimeLife had eight of these research Work Packages:

- WP2.1 is concerned with cryptographic mechanisms,
- WP2.2 works on mechanisms supporting privacy and trust,
- WP2.3 deals with privacy of data,
- WP2.4 researches access control for the protection of user-generated content,
- WP4.1 is about UI representation of privacy-enhancing IdM concepts,
- WP4.2 works on trust and assurance HCI,
- WP4.3 is concerned with user interfaces for policy display and administration,
- WP5.2 focuses on research on next generation policies.

Detailed reporting on the research topics and results may be found within the research reports also referencing the scientific publications produced. Activity 2 reported 22 publications from the research Work Packages of Activity 2 for the first period (see D2.1.1 First Report on Mechanisms), 32 papers for the second period (see. D2.3.1 Second Report on Mechanisms) and 46 publications in the last period (see. D2.4.1 Final report on Mechanisms).

Standardisation

Standardisation efforts in PrimeLife have widened their scope. At the beginning, we mainly target the International Standardisation Organisation (ISO), the UN-Internet Governance Forum (IGF) and the World Wide Web Consortium (W3C). During the project's lifetime we were participating and actively driving the PRIMCluster group, a group of other EU IST FP7 projects with similar standardisation targets. Furthermore, the decision for XACML as the main target language of the project put a new and strong focus on the cooperation with OASIS that was already successfully started.

ISO/IEC JTC 1/SC 27/WG 5 was working on a number of standards relating to PrimeLife activities. To the May 2009 meeting of ISO/IEC JTC 1/SC 27 in Beijing PrimeLife prepared and presented comments on and input to primarily the 6th WD of (24760) "A framework for identity management". During the meeting, an employee of one of the PrimeLife partners was appointed co-editor of this standard.

To the ISO/IEC JTC 1/SC 27 November 2009 meeting in Seattle further comments and input to the CD (24760) "A framework for identity management" was prepared and presented. Besides the comments presented PrimeLife also took active part in the discussions, the adHoc groups and the other work carried out during the meetings. PrimeLife partners GUF, KAU, GD and ULD participated in the ISO/IEC JTC 1/SC 27/WG 5 meetings in Beijing May 2009 and Seattle November 2009. The work then concentrated on analysing and commenting standards for the ISO/IEC JTC 1/SC 27 meeting in April 2010. During the ISO/IEC JTC 1/SC 27/WG 5 meetings in Singapore (April 2011), both the Privacy Framework (ISO 29100) and the Framework for Identity Management (ISO 24760-1) could conclude their core work and move those projects to the status of Final Draft International Standard, where they are now being balloted. During this stage only editorial changes will appear, thus two central projects could be successfully be progressed during PrimeLife's Lifetime. However, much of the remaining ongoing work will be taken up and continued by the ABC4Trust project.

W3C continued the dialogue with relevant stakeholders in the area of policy language via the PLING Working Group. PLING was mainly instrumental in organising the W3C Workshop on Access Control Application Scenarios²¹. The Workshop was chaired by the chair of OASIS TC XACML, Hal Lockhart from Oracle in Boston. The Workshop gathered people from research and industry together to discuss new uses and potential shortcomings in access control. As XACML is a language widely used, most papers and input to the workshop was referring to it. However, the discussion weren't strictly limited to XACML. There was some focus on using XACML to implement privacy friendly identities management, but the variety of use cases and papers submitted let to a more general discussion. As a result, the Workshop identified extension points for XACML. Via PLING and PRIMCluster feedback was provided into OASIS TC XACML of works going on in PrimeLife, TAS3, SWIFT and PICOS. It has to be noted that the cooperation with NESSI and the people around cloud computing, Software and

²¹ <http://www.w3.org/2009/policy-ws/>

Services did not work. Despite promises, nobody from the SOA/Cloud/SAS community sent a position paper or attended the Workshop.

There were large discussions with the W3C Geolocation Working Group about privacy requirements for the use of geodata on the web via the geolocation API. This has led to an improvement of the privacy and security considerations in the W3C Working Draft, but it is not satisfactory yet. Further work is expected on the deliverables of the W3C Device API Working Group. At the same time, PLING was used as a platform to coordinate and give input to the Mozilla project on privacy interfaces and requirements. At meeting at the W3C Technical Plenary in Santa Clara was used to reach out to OpenID and the Social Networking Community.

PrimeLife and Open Source

The aim of PrimeLife was to make Privacy real, which required supporting and triggering a broad uptake of privacy-enhancing solutions for IdM developed by PrimeLife. To achieve broad acceptance and roll-out of PrimeLife results, the project aimed at ensuring that the community at large adopts privacy technologies. One of the means towards this goal was PrimeLife's contribution of results to the community as open source. PrimeLife has produced thirteen components that have been released to the public via www.primelife.eu and other appropriate developer sites such as SourceForge.net, freshmeat.net and alternativeTo.net. Apart from that, PrimeLife also maintains and has extended the results from the PRIME project. For a comprehensive overview including a brief descriptions of the components and what they as well as the impact please refer to PrimeLife Deliverable "D3.3.2 Open Source Impact", available at <http://www.primelife.eu/>.

- Dudle
- Over-Encrypt
- Pri-views
- Identity Mixer Crypto Library (idemix)
- Identity Mixer Policy Engine
- Scramble!
- Clique
- Privacy-Oriented Tagging for Clique
- Privacy Enhancing Browser Extensions (Privacy Dashboard)
- PRIME Core
- MediaWiki/phpBB – Privacy Enhanced Access Control
- MediaWiki – Reputation Extension
- phpBB Privacy-Awareness Support: Personal Data MOD

As described in Deliverables D3.4.2, H3.3.2 and D3.3.2 there are several Open Source projects to which PrimeLife was related. PrimeLife did not have the resources to integrate its results into specific projects. Still, PrimeLife supported contacts with a number of these projects and PrimeLife presented them our results. In a number of cases PrimeLife results are based on Open Source projects, i.e., we have extended these with privacy-enhancing mechanisms (e.g., Elgg and phpBB). PrimeLife intensified the contact with these projects and offered them these extensions. Such collaboration with the open source maintainers took place for "Clique" with regard to Elgg, the social networking platform on which Clique is based. Clique provides users with a social network platform that enables them to keep control over their privacy. This includes, for example fine grained access control and configuration of multiple faces (e.g. family, personal, professional) that can be used for interactions with other users. Furthermore, "Scramble!" resulted out of the collaboration. Scramble! ("Scramble your social network data"). With "Scramble!" the user can selectively enforce his access control preferences for his content on social networks like Facebook or Twitter. The Privacy Enhancing Browser Extensions, or "Privacy Dashboard" in short, are extensions for the widespread Firefox browser. The extensions have been introduced at several conferences targeting the web 2.0 community, particularly towards developers. As far as it can be assessed by time of the editorial deadline, there had been a great interest and much is expected for the Federated Social Web Summit Europe in June 2011.

The components with relation to anonymous credentials, namely Identity Mixer Crypto Library and Identity Mixer Policy Engine have been released und open source licenses as well. Identity mixer will be used in a number of new research projects including the following EU funded ones ABC4Trust (realising to pilots – abc4trust.eu), di.me

(identity management – dime-project.eu), and FI-Ware (which builds the future internet infrastructure – fi-ware.morfeo-project.org).

For more details and the other PrimeLife open source results please refer to the dedicated PrimeLife deliverable "D3.3.2 Open Source Impact".

PrimeLife Book

The PrimeLife book contains the main research results from the PrimeLife Activities. It has been published with Springer and was available at the PrimeLife Summit Event. It addresses primarily researchers. In addition to fundamental research it contains descriptions of best practice solutions.

The PrimeLife book had been edited with the help of all activity leaders, who have been responsible for filling parts dedicated to their activities with material presenting the main Activity research results.

The PrimeLife book is structured as follows:

Introduction (basic definitions, setting the scene)

Part 1: Privacy in Life (Activity 1)

Part 2: Mechanisms in Privacy (Activity 2)

Part 3: HCI (Activity 4)

Part 4: Policy Languages (Activity 5)

Part 5: Infrastructures for Privacy and Identity Management (Activity 6)

Part 6: Privacy Live

Book chapters have been reviewed by a review board consisting of members of the PrimeLife project and the PrimeLife Reference Group.

PrimeLife Workshop Series

PrimeLife has promised and subsequently organised several different kinds of workshops to disseminate results and to get feedback on ongoing research tasks:

- Workshops for the PrimeLife Reference Group that gave feedback on results achieved by PrimeLife results during the project's lifetime ("Reference Group Meetings");
- Summer Schools for researchers and students that taught about state-of-the-art and new results and trends on privacy-enhancing identity management;
- Standardisation Workshops that addressed standardisation initiatives;
- Workshops for journalists to explain PrimeLife's results and position the project in the identity management landscape;
- Cooperation Workshops for related projects, interested developers or other parties who discussed their own needs for PET modules and picked up PrimeLife's results to improve their own concepts and IT systems. Similar other projects and potential follow-up projects that could profit from the technical expertise gained within PrimeLife have been addressed.

The workshops function as interaction means with relevant stakeholders grouped by their main interest. Per workshop the appropriate PrimeLife partners were asked to present recent project results and to elicit the desired feedback on currently open research questions.

From the experience within PRIME the partners have learned that other EC-funded projects as well as national projects have a great demand for knowledge and experience on privacy legislation and privacy technology. To meet these demands, PrimeLife has held and organised "Cooperation Workshops" where mainly specific questions of interested projects or institutions were discussed. By this means, PET ideas, technical solutions or legal concepts developed within PrimeLife were tailored according to the needs of the audience. The following consortia of projects have stated their interest in such a cooperation or have subsequently participated in some kind of joint activity with PrimeLife: ABC4Trust, AVANTSAR, Daidalos, Daidalos II, DESIRE, di.me, Effectsplus, EnCoRe, ENDORSE, ETICA, FIDIS, GeoPKDD, Liberate, MOBIO, NESSOS, PEACE, PEGASO, PETweb, PETwebII, PICOS, PrivacyOS, SEMIRAMIS, SEPIA, SeVeCom, SMILE; TURBINE and VESUV.

Besides other ICT or privacy related projects on European or national level some target audiences have been identified that might particularly benefit from PrimeLife knowledge or are notably disseminators. These include inter alia

- Journalists, especially those specialised in information and communication technologies, could help to spread information about the PrimeLife project and its results to the public and to special interested groups. In

particular, results that are also of interest for the general public are adequate including the research related to social networks or the publicly available extension for the Firefox browser "PrimeLife Dashboard".

- Price comparison services might be convinced to include information about the privacy policies of the webshops into the comparison tables as it is done with information on payment options or costs for package already. Ideally, this could result in a competitive advantage for market participants deploying privacy-enhancing technologies and solutions and subsequently may convince webshops to implement clear and understandable, preferably even computer readable, privacy policies to allow comparison as well as PETs. This may directly lead to more privacy protection for a broad number of users. ULD therefore developed a concept for micro workshops targeting price comparison agents. At the time of the editorial deadline of this report ULD was still in negotiation with several price comparison agents
- Stakeholders and researchers in the area of eHealth in general and personalised health monitoring in particular started to realise the privacy implications within their work. PrimeLife's specific results related to requirements for lifelong privacy are highly relevant within this area. Relevant PrimeLife content includes the basics about privacy throughout life and during periods of life with reduced capabilities to take care of one's own private sphere, delegation of data subject's rights as a potential solution also the privacy protection goals as described in D6.3.1.
- Addressing developments in the web 2.0 environment a rather heterogeneous community of stakeholders needs to be addressed consisting inter alia of developers, service providers, privacy, and security experts, advocates entrepreneurs in the space of social web and users. Since PrimeLife partner W3C was being involved with organising the Federated Social Web Summit held in Portland 2010 it seemed appropriate to address the same community now focussing more on privacy and security issues as have been focal point within PrimeLife research. In consequence, PrimeLife the Federated Social Web Europe conference had been planned and held.

The idea of promoting PrimeLife-based solutions in workshops is a specific approach in PrimeLife. The workshop series aims at two possible benefits: direct feedback to the researchers and direct communication to inform and convince target audiences. To successfully reach target audiences within the workshop series, some workshops have been focused on the topics of special interest for the targeted audience. We believe that such tailored (micro-) workshops may have a better impact as the addressed persons are given the opportunity to discuss their specific issues with the researchers. However, for larger events such as the Summer Schools, the Reference Group meetings and the Summit Event the full spectrum of PrimeLife topics had been available addressing inter alia the whole privacy and security communities.

PrimeLife Reference Group Meetings

The PrimeLife project established an external expert panel, the Reference Group, which consisted of representatives of relevant stakeholders: consumer organisations, data protection authorities, industry, academia, NGOs, and EC authorities. The PrimeLife Reference Group has been established to receive early review of project results and collect feedback from experts before a wider audience was addressed. However, the goal of the workshops with the Reference Group was to receive their comments and advise on currently open research questions in the project. By means of this approach quality assurance for past work, as well as guidance for future steps was sought by the consortium. Two meetings of the Reference Group were planned within the project's lifetime. Finally, some experts also joined the Summit Event also presenting PrimeLife from the viewpoint of the Reference Group. Besides the meetings, there was a close cooperation between the project's researcher and relevant experts. The Reference Group consisted of 26 members – the group was dynamic and some new members also were invited throughout the project lifetime.

First Reference Group Meeting

The First Reference Group Meeting was held from March 23rd to 24th 2009 in Frankfurt, Germany with 14 members attending. The two day meeting has been organised in six sessions. These sessions were opened by a presentation held by the activity and work package leaders giving the Reference Group a thorough overview of the planned work, achieved results and open research questions. Following the presentations, open discussions allowed collecting comments and advice from the external experts. Each day has been concluded with a short wrap up session.

From the project's side, all activities were represented by the activity leader or a proxy. Other participants were work package leaders within PrimeLife presenting on their specific area of research or were responsible for the logistical and financial organisation of the Reference Group meeting.

The venue at Frankfurt was kindly organised and provided by the PrimeLife partner Goethe University Frankfurt (GUF) on the University's "Campus Westend" which was formerly built as the representative seat and administrative centre of the IG Farben. The meeting room "Paris" is located in the newly build House of Finance. The agenda of this meeting is listed below.

Welcome, introduction of PrimeLife

First session: HCI and Trust

- Policy management in HCI
- Trust evaluation
- Discussion

Second session: Policies, Standards and Open Source

- Policy language
- Policy enforcement
- Policies and service composition
- Open Source approach
- Standardisation
- Outreach and networking
- Discussion

Third session: Trusted content and privacy for life

- Linkage and data aggregation over lifetime
- Revocation of identities
- Delegation
- Trust and nomadic devices
- Discussion

Fourth session: Social Network services

- Legal aspects
- Social aspects
- Discussion

Fifth session: Mechanisms

- Mechanisms supporting user's privacy and trust
- Access control for the protection of user-generated data
- Privacy of data
- Discussion

Sixth session: Infrastructure

- Trusted infrastructure elements
- Service composition
- Discussion

The meeting was chaired by Marit Hansen (ULD) who is responsible activity leader for the dissemination work package. The Feedback of the Reference Group with regard to the sessions is in detail presented in the report "D3.1.4 Summary of Reference Group Feedback".

Second Reference Group Meeting

The Second PrimeLife Reference Group Meeting was also held in Frankfurt, Mach 29th to 30th with 17 members of the Reference Group attending. PrimeLife partners used this meeting to present current results and to get direct feedback from the Reference Group Members. Work package and activity leaders gave a detailed overview on the

ongoing work and results, so the Reference Group members got an impression about the current problems and results of the project.

As the organisational feedback of the first Prime Life Reference Group Meeting was very positive, also the second PrimeLife Reference Group Meeting took place at the Prime Life partner Goethe University Frankfurt (GUF).

The meeting has been organised in seven sessions. Each session had a responsible PrimeLife activity or work package leader as a moderator who presented the theme and results and guided the discussion. Each day was concluded with a joint wrap up session with all participants.

The agenda of this meeting is listed below.

Welcome, introduction of PrimeLife

Brief introduction of PrimeLife

First session: HCI and Trust

- HCI for Credential Selection
- HCI for Data Track
- HCI for Policy Display and Management (and Policy Icons)

Second session: PrimeLife Prototypes

- Clique
- Scramble
- phpBB

Third session: PrimeLife Prototypes

- Data track/Transparency Tools
- MediaWiki

Fourth session: Privacy throughout life

- Report from the use case and requirement analysis
- Presenting the prototype mockups
- Report from the delegation aspects (legal)

Fifth session: Policies

- Policy research
 - Credential-based access control
 - Policy sanitization
 - Downstream usage control
 - Policy icons
- Policy implementation
 - Language
 - Engine
- Standardisation

Sixth session: Mechanisms

- Brief Crypto Notes: Oblivious Access Control
- Tools from WP 2.2

Fourth session: Infrastructures

- Presentation and Discussion of D6.1.1
- Demo of eCV Scenario
- Presentation and Discussion on WP 6.2 Demonstrator: Approach, Storyboard, Technologies

Overall Summary of the Reference Group Meetings

PrimeLife Work Package and Activity Leaders used the opportunity on the Reference Group Meetings to gain expert feedback on results and ongoing research in PrimeLife. The Reference Group members on each Reference Group Meeting got first of all a detailed impression into work ongoing in PrimeLife. Activity and work package leaders gave the Reference Group a thorough overview of the planned work, achieved results, and open research questions. Following the presentations, open discussions allowed collecting comments and advice from the external experts. Catering for breaks was available in a separated lobby of the meeting room allowing continuing and intensifying discussions.

The overall feedback of the Reference Group in both Reference Group Meetings was very positive towards the existing results presented and the research directions taken by the project. The Group pointed the researchers of the project to open issues and proposed approaches for solutions yet to be verified. In addition, the importance of further communication with specific interest groups such as open source communities related to PrimeLife's development of prototypes was highlighted.

As a follow up, the Reference Group Members stayed in close contact to PrimeLife Work Package and Activity Leaders even after the end of the Meetings, to further help and guide them through the discussed points within the Meeting. In conclusion, the Reference Group could –during the meetings and as required- contribute actively in the project's discussions and ongoing work. Members of the Reference Group themselves gave their specific input and feedback on the results of PrimeLife and therefore validated requirements and supported project dissemination and exploitation.

PrimeLife/IFIP Summer Schools

During the lifetime of the project PrimeLife organised two summer schools. Task 3.2.1 had been led by Karlstad University who had comprehensive experience in organising summer schools for PRIME and FIDIS jointly with IFIP (International Federation for Information Processing). IFIP is an ideal cooperation partner, as like PrimeLife, it also takes a holistic approach to technology and supports interdisciplinary exchange. Besides, it can as the umbrella organisation of national computer societies help to address the broader international IFIP and research community.

The aim of the Summer Schools is to encourage young academic and industry entrants to the privacy and identity management world to share their own ideas and to build up a collegial relationship with others, and in particularly disseminate research results from PrimeLife and related projects to young PhD students and industry entrants.

The school is interactive in character, and is composed of both, keynote lectures and seminars, tutorials and workshops with PhD student presentations. Keynote presentations by senior PrimeLife researchers and researchers from related projects were invited and were given in the morning sessions. The keynotes provided for an excellent platform for disseminating PrimeLife thinking. Keynote speakers came inter alia from the industry sector (IBM, Microsoft, Intel, Google, GD, Symantec), research (Institute Eurecom, the Swedish Royal Institute of Technology), universities (Dresden, Leuven, Tilburg, London) the governmental sector (The White House, German Ministry of Interior) and data protection authorities (CNIL). Besides students, the keynote speakers were regular part of the audience and many of them joined the whole week, encouraging deeper discussions with students and junior researches. Other EC-funded projects presented results and discussed open research questions – both of the PrimeLife and their own projects. The EC-funded projects PICOS, Turbine, Safebook, TAS3 and ETICA, were represented as well as the British EnCore, the Norwegian Petweb II project and the international PeerSoN project. In respect to the geographic origin the participants came from 11 EC-countries including some of the younger member states (Czech Republic, Slovakia, Slovenia) as well as six non-EC countries (Brazil, India, Canada, US, Norway and Switzerland).

In the afternoons, there were parallel workshops, in which PhD students can present their work and discuss it with other PhD students and senior researchers. Abstracts for workshop presentations by PhD students were solicited by a Call for Contributions that is circulated well ahead of the Summer Schools. Contributions were selected based on an extended abstract review by a Summer School Programme Committee.

Accepted short versions of papers were made available to all participants in the Summer Schools Pre-Proceedings. After the summer Schools, authors had the opportunity to submit their final full papers (which address include questions and aspects raised during the Summer School) for publication in the Summer School Proceedings published by the official IFIP publisher Springer. The papers to be included in the Final Proceedings published by Springer in spring/summer of the following year have again be reviewed and selected by the Summer School Programme Committee.

PrimeLife/IFIP Summer School 2009 in Nice, France

From 7th-11th September 2009, PrimeLife WP 3.2 held the first PrimeLife Summer School in cooperation with IFIP working groups 9.2 (Computer and Social Accountability), 9.6/11.7 (IT Misuse and the Law), 11.4 (Network Security) and 11.6 (Identity Management) in Nice/France with SAP Research as the local organiser.

The theme of the PrimeLife/IFIP Summer School 2009 was on "Privacy and Identity Management for emerging Internet Applications throughout a Person's Life".

The proceedings of the 2009 Summer School have been published by Springer in June 2010.

The following persons from PrimeLife and IFIP were involved in the Summer School's organisational and programme committee work:

General Chair:

Michele Bezzi (SAP Research/France)

Programme Committee Co-Chairs:

Penny Duquenoy (Middlesex University/ UK, IFIP WG 9.2 chair)

Simone Fischer-Hübner (Karlstad University/ Sweden, IFIP WG11.6 vice chair)

Marit Hansen (Independent Centre for Privacy Protection Schleswig-Holstein, Kiel/ Germany)

Organising Committee Chair:

Jean-Christophe Pazzaglia (SAP Research/ France)

PrimeLife/IFIP Summer School 2010

After the success of the 2009 PrimeLife/IFIP Summer School, PrimeLife and IFIP (International Federation for Information Processing, Working Groups 9.2, 9.6/11.7, 11.4, 11.6) continued their joint cooperation. The Summer School was held in Helsingborg in Southern Sweden, 2-6 August 2010. The topic had been "Privacy and Identity Management for Emerging Internet Applications throughout a Person's Life".

A special one-day stream within the Summer School, to which abstracts/papers could be submitted directly, had been organised by the EU FP7 project ETICA on privacy and related ethical issues arising from emerging information and communication technologies. Apart from that, the established and successful structure and scope of the 2009 Summer School had been kept. In particular, the school was again interactive in character, and was composed of both, keynote lectures and seminars, tutorials and workshop with PhD student presentations. Contributions had been selected based on an extended abstract review by the Programme Committee, consisting of senior IFIP and PrimeLife project members.

Accepted short versions of papers have been published in the Summer School Pre-proceedings. After the Summer School, participants and keynotes submitted their final papers for the Final Summer School Proceedings to be published by Springer in 2011. These papers had again reviewed by the Programme Committee. The Proceedings of the Summer School 2010 have been published by Springer in May 2011.

The 2010 Summer School had been chaired by the following persons from PrimeLife and IFIP:

General Chair:

Simone Fischer-Hübner (Karlstad University / Sweden)

Programme Committee Co-Chairs:

Penny Duquenoy (Middlesex University / UK)

Marit Hansen (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel / Germany)

Ronald Leenes (Tilburg University / Netherlands)

The call for papers has been published in February 2010. The Summer School websites are available at:

<http://www.it.kau.se/IFIP-summer-school/>

Supporting the IFIP Summer School 2011

After the success of the privacy centred Summer Schools PrimeLife has a major interest in ensuring the sustainability of the Summer School series. For this, the PrimeLife project supported planning and organisation of the IFIP Summer School 2011 which will be held in Trento, Italy and address the topic of "Privacy and Identity Management for Emerging Internet Applications throughout a person's lifetime". As the actual event will take place from September 5th to 9th and thus after the official end of the project PrimeLife is not possible to support the event with funding. However, PrimeLife partners have been highly encouraged to submit contributions and to perceive the Summer School as a possibility to communicate project results towards the current and future privacy projects. In particular, the European projects ABC4Trust, Endorse and NESSOS as well as the Norwegian PETweb II and Swedish U-PrIm projects may be addressed, as these are cooperating with the Summer School.

The 2010 Summer School will be chaired by the following persons from PrimeLife and IFIP:

General Summer School Chair:

Bruno Crispo (University of Trento, IT)

Marc van Lieshout (TNO, NL)

Programme Committee co-Chairs:

Jan Camenisch (IBM Research – Zurich, CH)

Simone Fischer-Hübner (Karlstad University, S)

Ronald Leenes (Tilburg University, NL)

Organising Committee Chair:

Giovanni Russello (Create-Net, IT)

The call for papers has been published in April 2010. The Summer School website is available at: <http://disi.unitn.it/security/ifip-summer-school2011/index.html>

Standardisation Workshops

The PRIME project already influenced standardisation in W3C and ISO. Three successful standardisation workshops had been held in 2006, 2007, and 2009. PrimeLife benefits from the PRIME partner's experience and will continue the efforts by organising workshops and meetings on standardisation.

In January 2009 W3C organised a **W3C Workshop on the Future of Social Networking**²² and Privacy was an important aspect of the discussion. PrimeLife partners TILT and W3C contributed Position papers: Privacy and Social Network Sites: Follow the Money!²³ from TILT and Semantic enhancements for social networks²⁴ from W3C. The Workshop Report²⁵ contains directions clearly influenced by the PrimeLife project. As a result of the W3C Workshop on the Future of Social Networking there is an initiative about creating a W3C Incubator Group for Social Networking. The ongoing effort for organisation can be followed on public-social-web-talk@w3.org²⁶. PrimeLife will further contribute to this effort as social networks are one of the core use cases of PrimeLife.

In 2009, W3C furthermore organised a **W3C Workshop on Access Control Application Scenarios**, see 0 above. People from research and industry discussed new uses and potential shortcomings in access control. As XACML is a language widely used, most papers and input to the workshop was referring to it. But the discussions were not strictly limited to XACML. There was some focus on using XACML to implement privacy friendly identities management, but the variety of use cases and paper submitted let to a more general discussion. As a result, the workshop identified extension points for XACML that are further detailed in the Workshop Report²⁷ that also

²² <http://www.w3.org/2008/09/msnws/>

²³ <http://www.w3.org/2008/09/msnws/papers/tilt.pdf>

²⁴ <http://www.w3.org/2008/09/msnws/papers/policy-ih-rw.html>

²⁵ <http://www.w3.org/2008/09/msnws/report>

²⁶ <http://lists.w3.org/Archives/Public/public-social-web-talk/>

²⁷ <http://www.w3.org/2009/policy-ws/report.html>

contains directions clearly influenced by the PrimeLife project. This first workshop on standardisation issues focused on the following core-activities:

- Thorough discussion on the status of policy languages from different perspectives
- Several Examples for applications were elaborated
- Further research areas identified.

The results of the above-mentioned workshops resulted in the **W3C Workshop on Privacy for Advanced Web APIs** in July 2010 in London to discuss the current work on the user facing side within a broader audience. This Workshop served to review experiences from recent design and deployment work on device APIs and to investigate novel strategies toward better privacy protection on the Web that are effective and lead to benefits in the near term. The results of the workshop can be found here: <http://www.w3.org/2010/api-privacy-ws/>.

Furthermore, W3C organised a follow-up **Workshop on Privacy and Data Usage Control** in October 2010 in Cambridge (MA) to encourage further discussions on the question of data usage once data has been collected. The results of the workshop can be found here: <http://www.w3.org/2010/policy-ws/>.

In December 2010, a workshop was co-organised with the Internet Architecture Board (IAB), W3C, the Internet Society (ISOC), and Massachusetts Institute of Technology (MIT): the **W3C Workshop on Internet Privacy** in Boston. A broader scope was chosen intentionally to discuss upcoming issues in online privacy that need to be tackled on a global scale. The results of the workshop can be found here: <http://www.iab.org/about/workshops/privacy/>.

In April 2011, the **W3C Workshop on Web Tracking and User Privacy** was held in Princeton. Position papers and results of the workshop are available at: <http://www.w3.org/2011/track-privacy>

In May 2011, the last of the workshops in PrimeLife's series dedicated to standardisation was held in Mountain View, USA. The **W3C Workshop on Identity in the Browser** addressed issues of Identity in the Browser. Position papers and results of the workshop are available at: <http://www.w3.org/2011/identity-ws/>

Last, but not least, although using a mix of approaches, the **Social Web Conference Europe held in June 2011** also included elements of a W3C workshop and was invited to paper submissions as such, which saw a significant number of contributions to establishing federation, privacy and security between social networking applications.²⁸

Workshops for journalists

On June 24th, 2011 PrimeLife held a workshop for journalists to explain the project's result and position the project in the identity management landscape. As the content that can be presented is heavily depending on the project's results this workshop is held at the end of the project. The workshops targeted journalists, junior-journalists and politicians. The workshop enabled the participants to evaluate whether websites collect information about visitors. Rigo Wenning from W3C demonstrated with the PrimeLife "Privacy Dashboard" how to make user tracking transparent. Subsequently Eva Schlehahn from ULD held a talk about the legal implications. It had been explained which rights tracking services violate and how users can defend their rights from a legal perspective. Finally, Rigo Wenning (W3C) and Ulrich König (ULD) guided the participants to use the "privacy dashboard" and gave some assistance to use it.

About 30 participants attended.

Cooperation Workshops

PrimeLife has made extensive use of the possibilities to network and disseminate results which are offered by the European Commission, e.g., by regularly attending conferences such as e-Challenges or the IST events. PrimeLife has furthermore contributed to the ICT event in September 2010 with several participants disseminating the project's research findings at this large and Europe's most visible forum for ICT research.

EC-funded projects approached PrimeLife to get consulting on specific questions regarding privacy and identity management. PrimeLife Partners have attended workshops of SWIFT, Daidalos II, TAS3, PrivacyOS, FIDIS, PICOS, NESSI, Think-Trust and several other projects to exchange knowledge and offer differing perspectives.

In addition various PrimeLife Partners have been actively taking part in workshops and working groups from ENISA, e.g., on reputation systems, social networks and privacy issues in the Ad-hoc Working Group "Privacy and Technology".

PrimeLife has been in contact with several European research projects, evaluating the possibility of holding joint workshops and discussing overlapping research topics. In addition, PrimeLife assisted other European projects in

²⁸ <http://d-cent.org/fsw2011/about/>

assuring privacy-enhancing identity management and other privacy enhancing techniques are considered and focused on. Projects and initiatives PrimeLife is in contact with include:

- ABC4Trust (Attribute-based Credentials for Trust; <https://abc4trust.eu/>)
- AVANTSSAR (Automated VALIDation of Trust and Security of Service-oriented ARchitectures; <http://www.avantssar.eu/>)
- CERP (Coordinating European Efforts for Promoting the European RFID Value Chain, RFID Cluster; <http://www.rfid-in-action.eu/cerp>)
- CONSEQUENCE (Context-aware data-centric information sharing; <http://www.consequence-project.eu/>)
- Daidalos II (Designing Advanced network Interfaces for the Delivery and Administration of Location Independent, optimised personal Services; <http://www2.inesporto.pt/utm-en/projects/projects/daidalos-ii-en/>)
- di.me (Integrated digital.me Userware for the Intelligent, Intuitive, and Trust-Enhancing Management of the User's Personal Information Sphere in Digital and Social Environments; <http://dime-project.eu/>)
- Effectsplus (European Framework for Future Internet Compliance, Trust, Security and Privacy through effective clustering; <http://www.effectsplus.eu/>)
- e-ME (Inclusive identity management in new social media; <http://e-me.no/>)
- EnCoRe (Ensuring Consent and Revocation; <http://www.encore-project.eu/>)
- ENDORSE (Legal Technical Framework for Privacy Preserving Data Management; <http://www.endorse-fp7.eu/>)
- ETICA (Ethical Issues of Emerging ICT Applications; <http://moriarty.tech.dmu.ac.uk:8080/>)
- EuroPriSe (European Privacy Seal; <https://www.european-privacy-seal.eu/>)
- FIDIS (Future of Identity in the Information Society; <http://www.fidis.net/>)
- MASTER (Managing Assurance, Security and Trust for sERvices; <http://www.master-fp7.eu/>)
- MOBIO (Mobile Biometry; <http://www.mobioproject.org/>)
- NESSI (Networked European Software & Services Initiative; <http://www.nessi-europe.com/>)
- NESSOS (Network of Excellence on Engineering Secure Future Internet Software Services and Systems; <http://www.nessos-project.eu/>)
- PETWeb II (Privacy-respecting Identity Management for e-Norge; <http://petweb2.projects.nislab.no/>)
- PICOS (Privacy and Identity Management for Community Services; <http://www.picos-project.eu/>)
- PrivacyOS (Privacy Open Space; <https://www.privacyos.eu/>),
- RESERVOIR (Resources and Services Virtualization without Barriers; <http://www.reservoir-fp7.eu/>)
- SecureChange (<http://www.securechange.eu/>)
- SEMIRAMIS (Secure Management of Information across multiple Stakeholders)
- SEPIA (Secure Embedded Platform with advanced Process Isolation and Anonymity capabilities; <http://www.sepia-project.eu/>)
- SSEDIC (Scoping the Single European Digital Identity Community; <http://www.eid-ssedic.eu/>)
- STORK (Secure idenTity acrOss boRders linked; <https://www.eid-stork.eu/>)
- SWIFT (Secure Widespread Identities for Federated Telecommunications; <http://www.ist-swift.org/>),
- TAS3 (Trusted Architecture for Securely Shared Services; <http://www.tas3.eu/>)
- Think-Trust (<http://www.think-trust.eu/>)
- TURBINE (TrUsted Revocable Biometric IdeNtitiEs; <http://www.turbine-project.eu/>)

PrivacyOS Meetings

PrimeLife attended the first Open Space conference of the EU funded project PrivacyOS in Strasbourg from October 13th to 15th 2008 and discussed with participants about actual privacy issues. Within the third PrivacyOS Conference on October 26th and 27th 2009 in Vienna, and the fourth PrivacyOS conference in Oxford on April 12th and 13th in Oxford, PrimeLife was also represented and got feedback on current work on privacy policies, usability, and the Privacy Dashboard. PrivacyOS is a European project aimed at bringing together industry, SMEs, government agencies, academia, and civil society to foster development of privacy infrastructures for Europe. Within the Open Space approach, all participants are invited to bring topics to the agenda. It leaves room for spontaneous creation of new workshops during the conference, which reflects the dynamics of the discussion among participants. The general objectives of PrivacyOS are to create a long-term collaboration in the thematic network and establish collective interfaces with other EC projects. Other projects present at the conference which

followed a workshop style were TAS3, SWIFT, EuroPriSe, and EnCoRe. PrimeLife partners IBM, ULD, GEIE ERCIM, and GUF participated in the conference. The positive experience led to also mix the Open Space approach into the mix of methods used for the Federated Social Web Europe Conference.

Joint PrimeLife, Daidalos II and SWIFT workshop

A joint workshop was carried out with the projects Daidalos II and SWIFT on October 23rd 2008 at the facilities of IBM Research Labs in Zurich. The workshop aimed at discussing a concept developed by Daidalos II for explicitly managing privacy, the so-called Virtual Identity (VID) concept. In addition, PrimeLife partners IBM and ULD made a high-level assessment based on an overview of DAIDALOS II obtained in this workshop with respect to privacy.

First PRIMCluster meeting

PrimeLife organised a cluster event of FP7 projects (PRIMCluster) together with the Commission as a joint workshop on February 25th 2009 in Brussels. The workshop comprised concrete technical discussions in the areas of overlapping interests of the projects, specifically identity management architecture, technologies and trust models, policies and Service Oriented Architectures. Projects joining this workshop were PICOS, TAS3, and SWIFT. PrimeLife partners IBM, EMIC, ULD and GUF participated in this workshop.

Session at the ICT event 2008 in Lyon

PrimeLife organised a session at the ICT event 2008 in Lyon on November 27th 2008 titled "Privacy Meets ICT Practice". The session was headed by PrimeLife Project Coordinator Dieter Sommer from IBM Zurich Labs and aimed at bringing together research projects with privacy challenges and other stakeholders. Presentations were given by representatives from the projects SWIFT, TAS3, CONSEQUENCE, and PrimeLife. PrimeLife partners IBM, TILT, G&D, EMIC, CURE, ULD, GUF, KUL, SAP, and GEIE ERCIM participated in the session, not all of them taking an active role.

Second PRIMCluster workshop

PrimeLife and the EC have co-organised the second PRIMCluster workshop to bring together the projects SWIFT, PrimeLife, and TAS3 in October 2009. This time, the focus of the discussions was the joint interest in policy languages, also in the light of an upcoming standardisation event on policies organised by PrimeLife. The meeting has taken place in Brussels, hosted by the European Commission. The third PRIMCluster workshop with participation of PrimeLife is already in preparation for May 6th, 2010 and will be held in Brussels. Topics will include network-level and application-level identity management and their relation.

Session at Service Wave conference

PrimeLife has co-organised a session with projects MASTER and TAS3 on November 23rd 2009 in Stockholm, co-located with Service Wave conference of November 23rd to 27th. The session was open to the public and titled "Identity Management in SOAs". PrimeLife partner IBM has been involved in the organisation of the session, partner GUF has attended the session.

PrimeLife workshop with STORK

On December 10th and 11th 2009, a workshop with STORK and PrimeLife has been held in Zurich, organised by PrimeLife partner IBM. The workshop has tackled privacy in STORK's eID interoperability framework. The inventors of the two prominent anonymous credential systems of today, Jan Camenisch and Stefan Brands, have attended the workshop. Concrete next steps for further collaboration have been envisioned, including proposals from the side of PrimeLife on how to bring stronger privacy to STORK.

Workshop on Policies for the Future Internet

Gregory Neven from IBM Research – Zurich represented PrimeLife at the "International Workshop on Policies for the Future Internet" that was held in Pisa, Italy, on February 5th, 2010. The workshop was meant to bring together a number of scientific presentations from various EC projects that have to deal with policy languages. Other EC projects represented at the meeting were TAS3, PICOS, Consequence, AVANTSSAR, Secure Change, and MASTER. Gregory Neven presented recent PrimeLife work on privacy extensions to XACML and SAML, which caused interesting and lively discussions on the card-based access control. Other interesting presentations included a presentation on distributed policy enforcement in XACML by David Chadwick from University of Kent and a presentation on usage control policies by Alexander Pretschner from Technical University Karlsruhe.

CERP – on the Internet of Things

PrimeLife was represented by the project partner K.U.Leuven in the Cluster of European Research Projects – CERP – on the Internet of Things. Within the scope of this involvement, K.U.Leuven participated in the meetings of the cluster. The Meeting in May 2009 resulted in the plan to write a Strategic Research Agenda on the Internet of things. A first version of the document, the CERP-IoT Strategic Research Agenda "Fall 2009" was produced in Q3 2009, with K.U.Leuven an active member of the Core editor team. "Internet of Things – Strategic Research Roadmap", 50p, IoT Cluster of European Research Projects, 15 September 2009, http://ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf. This piece of work had been presented to a multitude of players, active in IoT. In Q1 2010, a revised CERP-IoT SRA position paper had been generated, based on the comments on this work, in order to prepare the Strategic Research Roadmap. Moreover, the cluster published a Clusterbook, which includes the Strategic Research Roadmap and one-pagers on all the projects involved in the Cluster and some related papers. A pdf version is available online: http://www.internet-of-things-research.eu/cluster_book.htm. New projects of FP7 Call 5 have joined the Cluster, and a new impulse have been given to it, focussing amongst others on sustained dissemination and more international cooperation.

Third PRIMCluster Workshop

PrimeLife has organised the third PRIMCluster workshop, hosted at the EC premises of the Trust and Security Unit in Brussels, Belgium, on May 6. The workshop has contrasted the approaches of network-level vs. application-level identity management – approaches pursued by different member projects of PRIMCluster. Furthermore, we discussed how the member projects could jointly proceed with standardisation of their results in the access control domain within the XACML framework. Finally, we spoke about the workshops on privacy APIs to take place in London in June 2010 and on data handling organised with the MIT.

Fourth PRIMCluster Workshop

The fourth and final PRIMCluster Workshop was organised by PrimeLife and held on September 10 in Vienna, Austria. The participants have discussed the CardSpace in the Cloud approach of TAS3 as well as how delegation can be incorporated. Further items being worked on were policy standardisation which was a theme that was of interest throughout the series of PRIMCluster workshops.

ISO workshop at IDMan 2010

As part of the IDMan 2010 which had been held in Oslo in November 2010, a small 3 hour workshop on ISO standardisation within the Identity management area was held. One aim of the workshop was to give PrimeLife's view on the standard and to get feedback from the audience regarding the current standard draft. The other aim was to get feedback from the participants regarding their view on the benefits of standardisation within the IdM area as a whole.

Because of the dual aim the workshop was divided into two parts. The first part was a presentation of the current ISO standard draft on an identity management framework and PrimeLife's view on that draft. During this presentation, the audience was asked to comment or give suggestions of improvements when the different parts of the draft were presented. In connection with this presentation also the SEMIRAMIS project presented an overview of their work within the area.

The second part of the workshop was a panel discussion on the benefits of standards within the identity management area. The panel consisted of three persons with experiences from academia, industry and the governmental sector. The discussion that took place during the panel gave a good insight into different views on the pros and cons of standardisation within IdM and pointed out things that should be standardised and things that should not be standardised.

CPDP 2011

An approach to reach policy makers was the Computers, Privacy & Data Protection Conference (CPDP) on January 25th to 27th, 2011 in Brussels. PrimeLife acted as partner and sponsor of the conference and disseminated own material. Marit Hansen (ULD) and several other PrimeLife colleagues represented the PrimeLife project and contributed with talks, as session chairs and panel members.

Federated Social Web Summit Europe 2011

On June 3rd to 5th 2011, the Federated Social Web Summit Europe 2011 conference for presenting results for distributed social networks was held. The Federated Social Web Summit Europe 2011 was supported and co-organised by the World Wide Web Consortium (W3C) and by PrimeLife. Initiative and some local facilitation was

brought in by the independent institute PerGlobal, which created and promoted the label “d-cent”²⁹ as a coined term for the conference. The three day open event on Social Web interoperability, standards and privacy was also supported by and hosted by the Heinrich-Böll-Foundation, Berlin. In summer 2010, the first Federated Social Web Summit had taken place in Portland (USA) to kick-start a test-case driven approach to getting the federated social web working. The Federated Social Web Summit Europe was the second summit in a loose series, and the first to have taken place in Europe. Over 150 international experts attended the three day event, which included keynote-talks, paper submissions and an OpenSpace, spanning from societal requirements to work on specifications as well as developing visions for the future of social networking infrastructures. The event was covered well in German media including television appearance (under preparation at the time of writing this report).³⁰

Joint workshop on attribute-based Credentials

In cooperation with the newly started EU-Project "Attribute-Based Credentials 4 Trust (ABC4Trust)" a joint workshop with PrimeLife had been held on June 10th, 2011 IBM Research Zürich. Content of the tutorial had been to explain the basics of the technology, its potential spheres of application for privacy-enhancing technologies and selected building blocks of the underlying cryptography. The tutorials had been given by expert researchers from Microsoft and IBM, presenting a common view on Privacy-ABC technologies that encompasses both the U-Prove and Identity Mixer technologies.

Workshop on eHealth and privacy

A key challenge is the protection of health data throughout a person's lifetime – whether those data are personal or more generic. Indeed, it may be necessary to extend this protection beyond a lifetime, as disclosure of the data could adversely affect the individual's family members, descendants, and social or racial groupings. PrimeLife therefore co-organised a workshop in eHealth related issues at Middlesex University on June 16-17, 2011.

Micro Workshops

As part of the PrimeLife workshop series ULD also planned several micro workshops. The concept behind these events had been to plan and offer individual meetings with stakeholders to disseminate results that are specifically tailored for the respective group of stakeholders. Micro workshops also contributed much to PrimeLife's cooperation activities, as they are an ideal for deeper discussions or knowledge transfer between related projects.

An approach that seemed promising to us had been to organise a **workshop addressing services offering price comparisons online**. Some of these services offer additional information about the compared online shops such as a rating calculated by votes of other users, information on available payment methods or availability of goods. This allows users to compare not only the price but also other factors of the online shops. This led to the idea that also information on the privacy policy of the target websites should be displayed allowing user to also decide on this criterion. By the time of the editorial deadline of this report negotiations for a consultation within June or July 2011 were pending.

PrimeLife partner ULD participated in the **ad-hoc working group of the German data protection agencies** which developed privacy guidelines for the deployment of the new German eID. These have been influenced by PrimeLife's policy research done in work package 5.2. The contribution consisted of several ULD internal workshops preparing position papers as well as meetings with representatives the national data protection agencies and of the Bundesverwaltungsamt, the authority responsible for the transformation of the privacy relevant aspects of the new German eID.

ULD hosted and organised a **workshop on Cyber-Physical-Systems** providing research results from PrimeLife's policy work package and privacy related input towards the participating project which is currently developing a research roadmap for Germany.

As part of the privacy for life activities ULD cooperated with several initiatives in the area of **eHealth**. During **working meetings with projects related to eHealth and personalised health monitoring**. These meetings have been organised and hosted by ULD. PrimeLife provided consultations out of the legal PrimeLife working group. Working sessions had been held together with the European PHM-Ethics project, the German group preparing a study on "Juristische Fragen im Bereich altersgerechter Assistenzsysteme" and the nationally funded project SmartAssist. The projects had shown interest in on PrimeLife's research on privacy protection goals and delegation in privacy matters.

Privicons Meeting

²⁹ www.d-cent.org

³⁰ <http://chaosradio.ccc.de/cr168.html>

On March 13th 2011 a workshop on privacy icons (Privicons) was held in Berlin and was hosted by PrimeLife at the premises of the Landesvertretung Schleswig-Holstein. Participants were PrimeLife partners and invited partners from universities and research. The current status of the development of the Privicons was discussed and the next steps had been discussed, in particular the plans to include the privacy icons into the web applications of a large player in the IT area.

With **open government data** gaining relevancy in the public debate PrimeLife was invited to cooperate in addressing the privacy issues related to opening government data. It did so, by partnering with KU-Leuven for a workshop in April³¹ and with the organisers of the OKon-conference in Berlin for a follow-up in June³². Both workshops aim at a specialized group of people and are geared towards allowing a first exchange on a yet to be well researched topic.

³¹ <http://www.lapsi-project.eu/ogdwshop>

<http://www.law.kuleuven.be/icri/pages.php?pid=96>

³² <http://www.e-demokratie.org/veranstaltung/okon-2011-offenes-wissen-offene-daten/>

A1, A2: Scientific publications & all dissemination events

The below table contains all dissemination events of PrimeLife, including scientific publications. The latter are journal articles and articles in proceedings. The table is replicated from PrimeLife documents D3.1.6 and H3.1.3.

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati: "Location privacy in pervasive computing", in Security and Privacy in Mobile and Wireless Networking (S. Gritzalis, T. Karygiannis, and C. Skianis, eds.), Troubador Publishing, 2008	2008	book contribution	print	International	R&D		UNIMI
C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati: "Managing privacy in location-based access control systems", in Mobile Intelligence: Mobile Computing and Computational Intelligence (L. Yang, A. Waluyo, J. Ma, L. Tan, and B. Srinivasan, eds.), John Wiley & Sons, Inc., 2008	2008	book contribution	print	International	R&D		UNMI
C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati: "A privacy-aware access control system", Journal of Computer Security (JCS), vol. 16, no. 4, pp. 369-392, 2008	2008	journal article	print	International	R&D		UNIMI
Jan Camenisch, Thomas Gross, Thomas Heydt-Benjamin: "Rethinking accountable privacy supporting services", ACM DIM 2008	2008	article in proceedings	print	International	R&D	26-50	IBM
Jan Camenisch, Thomas Gross: "Efficient attribute encoding for anonymous credentials", ACM CCS 2008	2008	article in proceedings	print	International	R&D	101-300	IBM
Jan Camenisch, Rafik Chaabouni, Abhi Shelat: "Efficient Protocols for Set Membership and Range Proofs", in Proceedings of Asiacrypt 2008, Springer Verlag, 2008	2008	article in proceedings	print	International	R&D	101-300	IBM
Jan Camenisch, Gregory Zaverucha: "Private Intersection of Certified Sets", to appear in Proceedings of Financial Cryptography and Data Security 2009	2008	article in proceedings	print	International	R&D	51-100	IBM
PrimeLife project presentation at the first European Privacy Open Space in Strasbourg, 2008	2008	talk	oral	Europe	R&D, mixed audience	26-50	IBM
PLING wiki	2008, ongoing work	online	online	International	R&D	51-100	W3C, ULD, IBM, UMI, UBG, GUF

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Marit Hansen: "Enhancing User-Centric Identity Management Systems", in: Stefanie Geuhs (ed.): Net-ID 2008-Konferenzband incl. CD	2008-03	article in proceedings	print	International	industry	101-300	ULD
Marit Hansen, Alissa Cooper, Ari Schwartz: "Privacy and Identity Management", in: IEEE Security & Privacy, Vol. 6, No. 2, March/April 2008, pp. 38-45	2008-03	journal article	print	International	R&D	>1000	ULD
Marit Hansen: "Enhancing User-Centric Identity Management Systems", Net-ID 2008, Basel, Switzerland	2008-03-03	talk	oral	International	industry	51-100	ULD
Marit Hansen: Participation in eID panel at CeBIT fair, Hanover, Germany	2008-03-07	talk	oral	National	industry	26-50	ULD
Meike Kamp, Maren Raguse "Orientierung ja, Überwachung nein – Location Based Services auf dem Prüfstand", CeBIT fair, Hanover, Germany	2008-03-08	talk	oral	National	general public	101-300	ULD
Press release and launch of PrimeLife website with news	2008-03-27	press release	online	International	general public	>1000	W3C
Press release: "Identitätsmanagement 2.0: Datenschutzkonzepte für soziale Netzwerke in Arbeit"	2008-03-27	press release	online	National	general public	>1000	ULD
Invited Lecture on Biometrics at PRISE Final Conference, Austrian Academy of Sciences, Wien	2008-04	keynote	oral	Europe	EC project	26-50	TUD
Invited talk at the First Future Internet Assembly, part of a panel discussion in the break out session on security: "Services from a Privacy Perspective"	2008-04-01	talk	oral	Europe	EU Commission	101-300	IBM
Invited talk at the First Future Internet Assembly, break out session: "A Privacy Perspective on Content"	2008-04-01	talk	oral	Europe	EU Commission	101-300	IBM, TILT
Martin Meints: "Der ePass – eine Sicherheits- und Datenschutzanalyse", at SICHERHEIT 2008, Saarbrücken, Germany	2008-04-02	talk	oral	National	R&D	51-100	ULD
Martin Meints, Marit Hansen: "Der ePass – eine Sicherheits- und Datenschutzanalyse", in: Ammar Alkassar, Jörg Siekmann (eds.): SICHERHEIT 2008 – Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Lecture Notes in Informatics, Volume P-128, Köllen Verlag, Bonn 2008, pp. 31-43	2008-04-02	article in proceedings	print	National	R&D	500-1000	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Kai Rannenber: "Legal & Security Issues in ICT The case of Multilateral Security in context-rich services", at Dnevi Slovenski Informatike (DSI 2008) (Annual Conference of Slovenian Informatics Society, Portorož (Slovenia)	2008-04-10	keynote	oral	National	R&D, industry, policy makers, government authorities	101-300	GUF
Karel Wouters: "The PrimeLife Project", at NESSI TSD WG Workshop on Privacy	2008-04-11	presentation	oral	Europe	EC project	11-25	KUL, IBM
Marit Hansen: "User-Centric Identity Management", at GI-Fachtagung Verwaltungsinformatik 2008, Potsdam, Germany	2008-04-11	talk	oral	National	R&D	26-50	ULD
Kai Rannenber: "Privacy and Security – Where are they heading? – Linkages between security and privacy", presentation at JNSA (JNSA Japan Network Security Association) & IPA (Information-technology Promotion Agency), Kikai-shinko-kaikan, Tokyo, Japan	2008-04-23	keynote	oral	International	industry, R&D, policy makers, government authorities	26-50	GUF
Marit Hansen: "The Future of Web Identity – Privacy Issues", at 2 nd European Identity Conference in Munich, Germany	2008-04-23	talk	oral	International	industry	51-100	ULD
Marit Hansen: "Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies", at PRISE Conference "Towards privacy enhancing security technologies – the next steps" in Vienna, Austria	2008-04-29	talk	oral	International	R&D	26-50	ULD
Aleksandra Kuczerawy: "On Requirements for Privacy for Life", at AdapID Workshop	2008-05-20	presentation	oral	Europe	R&D	11-25	KUL
Maren Raguse "Datenschutz in Online Communities", lecture at Christian-Albrechts Universität Kiel, Germany	2008-06-04	talk	oral	National	general public	26-50	ULD
S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati: "Controlled information sharing in collaborative distributed query processing", in Proc. of the 28th International Conference on Distributed Computing Systems (ICDCS 2008), (Beijing, China), June 2008	2008-06-17	article in proceedings	print	International	R&D		UNIMI, UNIBG
Ulrich Pinsdorf: "Delegation of Access Rights in Multi-Domain Service Compositions", talk held at CAST-Forum Workshop on SOA Security	2008-06-19	talk	oral	National	R&D	51-100	EMIC

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Presentation by Jan Camenisch on PrimeLife held at the PRIME Closing Event, Leuven, Belgium	2008-06-21	presentation	oral	International	EC project	51-100	IBM
Privacy Aspects of Social Networks, discussions at the Schleswig-Holstein-Tag, Neumünster, Germany	2008-07-12	talk	oral	National	general public	51-100	ULD
C. Ardagna, S. De Capitani di Vimercati, T. Grandison, S. Jajodia, P. Samarati: "Regulating exceptions in healthcare using policy spaces", in Proc. of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, (London, U.K.), July 2008	2008-07-13	article in proceedings	print	International	R&D		UNIMI
Marit Hansen: interview with newspaper Frankfurter Neue Presse on "Soziale Netzwerke sind Fundgruben für Spammer"	2008-07-18	interview	online	National	general public	>1000	ULD
Kai Rannenberg: "Privacy & Multilateral Security in Mobile Communications", at International School on Foundations of Security Analysis and Design (FOSAD), Bertinoro, Italy	2008-08-25/26	presentation	oral	International	R&D	51-100	GUF
Three PhD talks (on awareness and privacy measurement) at IFIP/FIDIS Internet Security and Privacy Summer School, Masaryk University Brno, September 1-7, 2008	2008-09	talk	oral	Europe	R&D	26-50	TUD
Keynote on reputation systems and multilateral security at IFIP/FIDIS Internet Security and Privacy Summer School, Masaryk University Brno, September 1-7, 2008	2008-09	keynote	oral	Europe	R&D	26-50	TUD
Franziska Pingel, Sandra Steinbrecher: "Multilateral Secure Cross-Community Reputation Systems for Internet Communities", talk held at conference DEXA TrustBus, Turin	2008-09	talk	oral	International	R&D	11-25	TUD
Fanziska Pingel, Sandra Steinbrecher: "Multilateral secure cross-community reputation systems", in Proceedings of Trust and Privacy in Digital Business, Fifth International Conference, TrustBus (S. F. S. Katsikas and A. Liroy, eds.), vol. 5185 of Lecture Notes in Computer Science, pp. 69-78, Springer, 2008	2008-09	article in proceedings	print	International	R&D	101-300	TUD
Invited Lecture on Biometrics at conference DEXA TrustBus, Turin	2008-09	keynote	oral	International	R&D	11-25	TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Andreas Pfitzmann: "Biometrics – how to put to use and how not at all? ", in Proceedings of Trust and Privacy in Digital Business, Fifth International Conference, TrustBus (S. F. S. Katsikas and A. Lioy, eds.), vol. 5185 of Lecture Notes in Computer Science, pp. 1-7, Springer, 2008	2008-09	article in proceedings	print	Europe	R&D	101-300	TUD
Maren Raguse, Harald Zwingelberg: "Selbstschutz, Identitätsmanagement im Netz", Sommerakademie 2008, Kiel, Germany	2008-09-01	talk	oral	National	general public	26-50	ULD
Hans Hedbom: "A Survey on Transparency Tools for Enhancing Privacy", at the IFIP/FIDIS Summer school, Brno/Czech Republic	2008-09-01	talk	oral	International	R&D	26-50	KAU
Kai Rannenber: "Mobile Identity Management – Trends and Business Factors", at FIDIS/IFIP Internet Security & Privacy Summer School , Brno, Czech Republic	2008-09-04	presentation	oral	International	R&D	51-100	GUF
Ronald Leenes: "Virtual communities, privacy and trust", keynote held at IFIP/FIDIS 2008 Summer School, Brno, Czech Republic	2008-09-05	keynote	oral	International	R&D	60	TILT
Invited talk of Pierangela Samarati on "Access Control Policies and Data Protection: Some Results and Open Issues", in 23rd International Information Security Conference (SEC 2008)	2008-09-09	keynote	oral	International	R&D		UNIMI
presentation of a position paper at ThinkTrust meeting, Paris	2008-09-09	talk	oral	Europe	EU Commission	11-25	IBM
Marit Hansen: "Neue Datenschutztechnik für neue Herausforderungen", at 13th Symposium on Privacy and Security "Informatik und Datenschutz im Widerstreit?" Zurich, Switzerland	2008-09-09	talk	oral	National	general public	51-100	ULD
Marit Hansen: Participation in Think-Trust Workshop, Paris, France	2008-09-10	conference session	oral	International	policy makers	26-50	ULD, IBM
Ronald Leenes: "Privacy & identiteit in sociale netwerken", at KNAW symposium 'Identiteit in Virtuele Werelden', Amsterdam	2008-09-18	keynote	oral	National	R&D	80	TILT

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Professor Installation Talk by John Sören Pettersson "Vem tar dina personuppgifter, och vad kan du göra åt det?" This talk referred heavily to PRIME and the on-going PrimeLife project. Karlstad University	2008-09-18	talk	oral	National	R&D, general public	51-100	KAU
Stephan Spitz: "PrimeLife – Privacy and Identity Management in Europe for Life", presentation held at the eSmart / WorldID Conference	2008-09-19	presentation	oral	International	general public	51-100	GD
Marit Hansen: "Identitätsmanagement – pro oder contra Datenschutz", at conference "Vom Volkszählungsurteil zum virtuellen Exhibitionismus – Wertewandel des Datenschutzes", Tutzing, Germany	2008-09-26	talk	oral	National	general public	26-50	ULD
V. Piuri, F. Scotti: "Image processing for fingerprint biometrics via low-cost cameras and webcams", in IEEE International Conference on Biometrics: Theory, Applications and Systems, (Washington DC, USA), September 29 - October 1, 2008	2008-09-29	article in proceedings	print	International	R&D		UNIMI
Marit Hansen, Andreas Pfitzmann, Sandra Steinbrecher: "Identity Management throughout one's whole life", in Information Security Technical Report (ISTR) Vol. 13, No. 2 (2008), Elsevier Ltd, Cambridge (UK), 83-94	2008-10-04	journal article	online	International	R&D	101-300	TUD, ULD
Reports on PrimeLife Liason by Kai Rannenber (GUF): SC 27 WG Meetings, Limassol, Cyprus, including meetings of Working Group 5 on Identity Management and Privacy Technologies	2008-10-06 to 2008-10-10	presentation	oral	International	standardisati on body	51-100	GUF, ULD, KU
Pierangela Samarati: "Privacy in Data Dissemination and Outsourcing", at 13th European Symposium on Research in Computer Security (ESORICS 2008)	2008-10-07	keynote	oral	International	R&D		UNIMI
C. Ardagna, A. Stavrou, S. Jajodia, P. Samarati, R. Martin: "A multi-path approach for k-anonymity in mobile hybrid networks", in Proc. of the International Workshop on Privacy in Location-Based Applications (PILBA 2008), Malaga, Spain, October 2008	2008-10-09	article in proceedings	print	International	R&D		UNIMI
Marit Hansen: "Privacy and user control – core to identity management", at Catalyst Conference, Burton Group, Prague, Czech Republic	2008-10-21	talk	oral	International	industry	101-300	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti: "A multi-biometric verification system for the privacy protection of iris templates", in Proc. of the International Workshop on Computational Intelligence in Security for Information Systems (CISIS'08), (Genoa, Italy), October 2008	2008-10-23	article in proceedings	print	International	R&D		UNIMI
Participation in the W3C PLING Reference Group Meeting	2008-10-23	conference session	oral	International	standardisation body	11-25	W3C, IBM, KU Leuven, EMIC, UNIMI, UNIBG
Invited talk, Simone Fischer-Hübner: "Privacy and Identity Management for Life", at the "Technikdagen" of SFIS (Svensk förening för informationsspecialister), Norrköping, Sweden	2008-10-23	talk	oral	National	R&D	51-100	KAU
W3C Technical Plenary & PLING F2F Meeting with PrimeLife	2008-10-23 to 2008-10-24	conference session	oral	International	standardisation body	26-50	W3C, ULD, IBM, UMI, UBG, GUF, EMIC, SAP
Ronald Leenes: "Understanding privacy & identity in social networks", keynote at Privacy in Social Network Sites conference, Delft, Netherlands	2008-10-24	keynote	oral/online	International	R&D	40	TILT
John Sören Pettersson: "When Little Brother is watching you it is time to ask: Who has the right to mediate personal data?", at eChallenges 2008, Stockholm, Sweden	2008-10-24	talk	oral	International	R&D	51-100	KAU
Marit Hansen: "Linkage Control – Integrating the Essence of Privacy Protection into Identity Management Systems", eChallenges 2008, Stockholm, Sweden	2008-10-24	talk	oral	International	R&D	26-50	ULD
Marit Hansen: "Linkage Control – Integrating the Essence of Privacy Protection into Identity Management Systems", in: Paul Cunningham, Miriam Cunningham (eds.): Collaboration and the Knowledge Economy: Issues, Applications, Case Studies, Proceedings of eChallenges 2008, IOS Press, Amsterdam 2008, pp. 1585-1592	2008-10-24	article in proceedings	print	International	R&D	>1000	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, P. Samarati: "Preserving confidentiality of security policies in data outsourcing", in Proc. of the Workshop on Privacy in the Electronic Society (WPES2008), (Alexandria, Virginia, USA), October 2008	2008-10-27	article in proceedings	print	International	R&D		UNIMI, UNIBG
Marit Hansen: "Meine Daten gehören mir!", at Phänomena-Mathewochen, Phänomena, Flensburg, Germany	2008-10-28	talk	oral	National	general public	11-25	ULD
Meike Kamp, MarenRaguse: "Kundendatenschutz, Datenschutz in Online Communities", lecture at University for Applied Sciences Flensburg, Germany	2008-11-05	talk	oral	National	general public	26-50	ULD
Marit Hansen: "Online Privacy", held at ESOMAR World Research Roundtable, Munich, Germany	2008-11-12	talk	oral	National	industry	26-50	ULD, IBM
Marit Hansen: interview with Heise on the occasion of ESOMAR World Research Roundtable, Munich, Germany	2008-11-12	interview	online	National	general public	>1000	ULD
Marit Hansen: "Data Protection – Situation and Challenges", held at Privacy Workshop, JRC Ispra, Italy	2008-11-14	talk	oral	International	policy makers	26-50	ULD
Kai Rannenberg: "Trends in Mobile Business & Marketing – Context is King, Privacy is Prince", at 2nd German Dialogue Marketing Congress, Kassel, Germany	2008-11-21	keynote	oral	National	industry, R&D	51-100	GUF
Participation and contribution to several session at ICT Lyon by PrimeLife partners	2008-11-24 to 2008-11-27	conference session	oral	Europe	R&D	51-100	W3C, IBM, GUF, GD, SAP
Talk at the networking session on policy modelling and simulation at the ICT 2008 Event. "Public Services: Privacy, Trust, and Modeling Challenges"	2008-11-25	talk	oral	Europe	R&D	26-50	IBM (ZRL in cooperation with IBM Germany)
Presentation on "A Trustworthy Information Society Privacy Protection and Identity Management", at Session on "A Trustworthy Information Society", at ICT Event 2008, Lyon, France	2008-11-26	presentation	oral	International	R&D, industry, EC projects, policy makers, journalists	101-300	GUF

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Invited panel presentation by Simone Fischer-Hübner at the ICT 2008, Lyon, 26th November 2008. Title of the talk: "Technology and Tools for Trustworthy ICT".	2008-11-26	talk	oral	International	R&D	101-300	KAU
Presentation on "Privacy meets (mobile) life", at PrimeLife Networking Session 107 "Privacy meets ICT Practice" Networking Session N. 107 at ICT Event 2008, Lyon, France	2008-11-27	conference session	oral	International	R&D, industry, EC projects, policy makers, journalists	51-100	GUF, IBM
S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati: "Assessing query privileges via safe and efficient permission composition", in Proc. of the 15th ACM Conference on Computer and Communications Security (CCS 2008), Alexandria, Virginia, USA, October 2008	2008-11-27	article in proceedings	print	International	R&D		UNIMI, UNIBG
PrimeLife organised a networking session at ICT 2008: "Privacy meets ICT Practice". http://ec.europa.eu/information_society/events/cf/item-display.cfm?id=653 Talks were on privacy-related projects, ongoing work, and challenges. The panel comprised both PrimeLife people and people from other projects (TAS3, SWIFT, CONSEQUENCE, PICOS).	2008-11-27	conference session	oral	Europe	R&D	51-100	IBM, ULD, EMIC
Talk at the ThinkTrust Networking Session "The impact of Trust, Security, Dependability, Privacy and Identity – Societal and ICT perspectives", at ICT 2008. Talk: "Privacy and Security – The Link to User-centric IDM"	2008-11-27	talk	oral	Europe	R&D	51-100	IBM
PrimeLife partners IBM, ULD, SAP, EMIC: participation at NESSI meeting, project presentation by D. Sommer, Lyon, France	2008-11-28	talk	oral	Europe	EC projects, R&D, industry	26-50	IBM, ULD, SAP, EMIC
Marit Hansen: "Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies", in: Johann Čas (ed.): D7.3 PRISE Conference Proceedings, pp. 91-103, 2008	2008-12	article in proceedings	online	International	R&D	>1000	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Contribution to NESSI privacy whitepaper	2008-12	position paper	online	International	EC projects, R&D, industry	>1000	IBM
Marit Hansen: "User-controlled identity management: the key to the future of privacy?", in: International Journal of Intellectual Property Management (IJIPM) Vol. 2, No. 4 (2008), Special Issue on Identity, Privacy and New Technologies, Part 2, pp. 325-344	2008-12	journal article	print	International	R&D	>1000	ULD
S. Cimato, M. Gamassi, V. Piuri, R. Sassi, F. Scotti: "Privacy-aware biometrics: Design and implementation of a multimodal verification system", in Proceedings of the Annual Computer Security Applications Conference (ACSAC24), Anaheim, California, USA, December 2008	2008-12-08	article in proceedings	print	International	R&D		UNIMI
Presentation of future research challenges in privacy-enhancing technology at ThinkTrust meeting, Madrid, Spain	2008-12-09	talk	oral	Europe	EU Commission	11-25	IBM
Claudia Diaz: "Security and Privacy Challenges in the Real World Internet", at FIA – Future Internet Assembly, Madrid, Spain	2008-12-09	presentation	oral	Europe	R&D	301-500	KUL
Marit Hansen: "Verkettung digitaler Identitäten in Wirtschaft, Verwaltung und Online-Communities", at Fachtagung Datenschutz der dbb Akademie, Cologne, Germany	2008-12-10	talk	oral	National	general public	51-100	ULD
Ronald Leenes: "Identity online, or how the market banks on social capital", lecture at the TILTING perspectives on regulating technologies conference, Tilburg, the Netherlands	2008-12-11	talk	oral	International	R&D	30	TILT
Marit Hansen: "Anforderungen des Datenschutzes an ID-Management in der medizinischen Forschung", at TMF-Workshop ID-Management, Berlin, Germany	2008-12-15	talk	oral	National	R&D	26-50	ULD
Harald Zwingelberg: "Identitätsmanagement, Anonymisierungsdienste", lecture on IdM at the University of Applied Sciences Kiel, Germany	2008-12-17	talk	oral	National	R&D	6-10	ULD
Several Teaching Lessons at GUF	2008-X all over the year	presentation	oral	International	government authorities		GUF

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Ronald Leenes: "User-centric identity management as an indispensable tool for privacy protection", in: Int. J. Intellectual Property Management, Vol. 2, No. 4, 2008, pp. 345-371	2009-01	journal article	paper	international	R&D, policy makers		TILT
Marit Hansen: "Datenschutz im Berufsalltag", held at BPW GERMANY Club Kiel e.V., Kiel, Germany	2009-01-06	talk	oral	National	general public	11-25	ULD
Position Paper for the Social Networking Workshop	2009-01-09	article in proceedings	online	International	R&D	301-500	W3C
Social Networking Workshop	2009-01-14 to 2009-01-15	conference session	online	International	R&D	301-500	W3C, TILT
Martin Pekárek, Ronald Leenes: "Privacy and Social Network Sites: Follow the Money", position paper for the W3C Workshop on the Future of Social Networking, Barcelona	2009-01-15	position paper	online	International	R&D		TILT
Ronald Leenes, SNS, about (re)discovering social norms and public goods, lecture at the international conference Computers, Privacy & Data Protection, 16-17 Jan 2009, Brussels.	2009-01-17	keynote	oral	International	R&D	80	TILT
Arnold Roosendaal: talk at the Tilburg Law Faculty's Research Day	2009-01-21	talk	oral	National	R&D, general public	51-100	TILT
"Identitätsmanagement – Notwendigkeiten und Grenzen eigenverantwortlichen Datenumgangs von Kindern und Jugendlichen", Symposium zum Europäischen Datenschutztag, Mainz, Germany	2009-01-28	talk	oral	National	general public	101-300	ULD
Maren Raguse: Interview with Deutsche Presseagentur (dpa) on Facebook's new Terms of Service, cited by over 90 online news websites	2009-02-17	interview	online	National	general public	>1000	ULD
C.A. Ardagna, J. Camenisch, M. Kohlweiss, R. Leenes, G. Neven, B. Priem, P. Samarati, D. Sommer, and M. Verdicchio: "Exploiting cryptography for privacy-enhanced access control: A result of the PRIME project". Journal of Computer Security (JCS), 2009.	2009	journal article	print	International	R&D	500-1000	IBM, UNIMI, TILT, KU, UNIBG

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati: "An obfuscation-based approach for protecting location privacy", in IEEE Transaction on Dependable and Secure Computing. pre-print.	2009	journal article	print	International	R&D		UNIMI
V. Ciriani, S. De Capitani di Vimercati, S. Foresti, P. Samarati: "Theory of privacy and anonymity", in M. Atallah and M. Blanton, (eds.), Algorithms and Theory of Computation Handbook (2nd edition). CRC Press, 2009.	2009	book contribution	print	International	R&D		UNIMI
C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, P. Samarati: "Access control in location-based services", in C. Bettini, S. Jajodia, P. Samarati, and S.Wang, (eds.), Privacy in Location Based Applications, Springer, 2009.	2009	book contribution	print	International	R&D		UNIMI
C.A. Ardagna, S. Jajodia, P. Samarati, A. Stavrou: "Privacy preservation over untrusted mobile networks", in C. Bettini, S. Jajodia, P. Samarati, and S. Wang, (eds.), Privacy in Location Based Applications. Springer, 2009.	2009	book contribution	print	International	R&D		UNIMI
B. Van Alsenoy, J. Ballet, A. Kuczerawy, J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?" in Identity in the Information Society (IDIS), 2009, special issue on Social Web and Identity	2009	journal article	print	International	R&D		KU
P. Guillemin, P. Friess, O. Vermesan, M. Harrison, H. Vogt, K. Konstantinos, M. Tomasella, S. Gusmeroli, K. Wouters, S. Haller: "Internet of Things – Strategic Roadmap", 43p, IoT Cluster of European Research Projects, 15 September 2009.	2009	brochure	online	International	EU Commission		KU
J. Camenisch, M. Dubovitskaya and G. Neven: "Oblivious transfer with access control", in E. Al-Shaer, S. Jha, and A. Keromytis, (eds.) Proceedings of the 2009 ACM Conference on Computer and Communications Security, pp. 131-140. ACM Press, 2009.	2009	article in proceedings	print	International	R&D	101-300	IBM
Jan Camenisch and Gregory M. Zaverucha: "Private Intersection of Certified Sets", in Proceedings of Financial Cryptography, p. 108-127, Springer LNCS, 2009.	2009	article in proceedings	print	International	R&D		IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Jan Camenisch, Markulf Kohlweiss, Alfredo Rial, and Caroline Sheedy: "Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data", in Proceedings of Public Key Cryptography (PKC) 2009, p. 196-214, Springer LNCS, 2009.	2009	article in proceedings	print	International	R&D	51-100	IBM
Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente: "An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials", in Proceedings of Public Key Cryptography (PKC) 2009, p. 481-500, Springer LNCS, 2009.	2009	article in proceedings	print	International	R&D	51-100	IBM
Giuseppe Ateniese, Jan Camenisch, Marc Joye, Gene Tsudik: "Remarks on "Analysis of one popular group signature scheme", in Asiacrypt 2006", in IJACT, Volume 1, Number 4, p. 320-322, 2009.	2009	journal article	print	International	R&D		IBM
Jan Camenisch, Sebastian Mödersheim, Gregory Neven, Franz-Stefan Preiss, Dieter Sommer: "Credential-based access control extensions to XACML", presentation at PrimeLife & W3C Workshop on Access Control Application Scenarios, Abbaye de Neumünster, Luxembourg	2009	conference session	oral	International	R&D, government authorities, industry, EC projects, standardisation body	26-50	IBM
Stephan Spitz, "Privacy on Mobile Devices: Present and Future Technologies", at ETSI Security Workshop in Sophia-Antipolis, France.	2009-01	presentation	oral	International	standardisation body	26-50	GD
Ronald Leenes: "Social Network Sites – about (re)discovering social norms and public goods", at Computers, Privacy & Data Protection 2010, Brussels, Belgium.	2009-01-16	talk	oral	international	R&D, industry, government	200	TILT
Stephan Spitz, Marc-Michael Bergfeld: "Creating Confidence in the innovation sphere of identity management and privacy protection", on Dissemination of news of the PrimeLife project through its internal website	2009-02	press release	online	International	industry	>1000	GD
Stephan Spitz: "Privacy on Mobile Devices: Present and Future Technologies", Embedded World in Nürnberg, Germany.	2009-02	presentation	oral	International	industry	26-50	GD
ThinkTrust meeting: Participation in discussions of the 2nd workshop of the ThinkTrust working group.	2009-02-24 to 2009-02-25	talk	oral	Europe	policy makers	26-50	IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Claudia Diaz, Eleni Kosta, Hannelore Dekeyser, Markulf Kohlweiss, Girma Nigusse: "Privacy preserving electronic petitions", in Identity in the Information Society, 1(1):14, 2009.	2009-02-25	journal article	print	International	R&D		KU
PRIMCluster meeting #1: Meeting between PrimeLife, SWIFT, TAS3, PICOS and the project officers thereof, exploring collaboration potential and overlapping/orthogonal interests and efforts, organised by EC and PrimeLife, multiple talks by PrimeLife.	2009-02-25 to 2009-02-26	talk	oral	Europe	EC project	11-25	IBM, ULD, KU, UNIBG, EMIC, SAP
Marit Hansen: "Informationen bei Datenschutzvorfällen: Ja, bitte!", in: DANA 1/2009, Bonn, pp. 12-13, http://www.datenschutzverein.de/Themen/dana/Hansen_Schuler_DANA0109.pdf	2009-03	journal article	print	National	general public		ULD
Jan Schallaböck: "PRM + Open Source = Transparenz für den Datenschutz?" Presentation at Heise CeBIT Forum, Hanover, Germany	2009-03-05	presentation	oral	National	general public	51-100	ULD
Interview with Marit Hansen, "Große Mehrheit sorgt sich um Privatsphäre im Netz", press publication, Germany	2009-03-16	interview	print	National	general public		ULD
1st PrimeLife Reference Group Meeting	2009-03-23 to 2009-03-24		oral	International	policy makers	11-25	IBM and most partners
Marit Hansen: "Großbritannien will soziale Netze überwachen", Interview and press publication	2009-03-25	interview	print	National	general public		ULD
Sebastian Meissner: Introduction of PrimeLife in the presentation "The European Privacy Seal (EuroPrise), goals and operation" at 3rd annual conference on personal data protection and data security in Palma de Mallorca (organiser: Balearic Islands Bar Association)	2009-03-27	presentation	oral	Europe	general public	26-50	ULD
Simone Fischer-Hübner: "Presentation about PrimeLife at Datainspektionen", Swedish Dataprotection Commissioner, Stockholm	2009-04-01	presentation	oral	National	government authorities	11-25	KAU
Filipe Beato: "Selective Access Control on Social Networks", 2nd PrivacyOS Conference, Berlin, Germany	2009-04-01 to 2009-04-03	talk	oral	International	R&D		KU
Katalin Storf, Jan Schallaböck: PrivacyOS Conference in co-location with re:publica conference, Berlin, Germany	2009-04-01 to 2009-04-03	workshop	oral	Europe	general public	51-100	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Rigo Wenning, Presentation of a privacy dash board at PrivacyOS meeting in Berlin	2009-04-01 to 2009-04-03	presentation	oral	International	R&D	26-50	W3C
Jan Schallaböck: "A Netiquette for Social Networks", Joint presentation at Re-Publica 2009 and 2nd European Privacy Open Space (together with Ralf Bendrath, and Prof. Hendrik Speck) in Berlin	2009-04-03	presentation	oral	Europe	general public	500-1000	ULD
Jan Schallaböck: "Demokratie und Datenschutz auf Facebook & Co", Interview published at futurezone.orf.at	2009-04-08	interview	online	National	general public	>1000	ULD
Ronald Leenes: "Privacy & identity in sociale netwerken", Introductiecollege UvT, talking to students and parents	2009-04-16	talk	oral	national	general public	200	TILT
Jan Schallaböck: "Datenschutzkontrolle durch Open Source", article published in: DuD 3/2009	2009-04-18	journal article	print	National	general public	500-1000	ULD
Jan Camenisch: "Identity, Trust and Privacy Management: State of the Art and Open Problems", presented at ZISC Information Security Colloquium, invited talk	2009-04-21	talk	oral	National	R&D	11-25	IBM
Jan Camenisch, Nishanth Chandran, Victor Shoup: "A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks", in Proceedings of EUROCRYPT 2009, pp. 351-368, Springer LNCS, 2009	2009-04-26 to 2009-04-30	article in proceedings	print	International	R&D	301-500	IBM
Jan Camenisch, Aggelos Kiayias, Moti Yung: "On the Portability of Generalized Schnorr Proofs", in: Proceedings of EUROCRYPT 2009, p. 425-442, Springer LNCS, 2009	2009-04-26 to 2009-04-30	article in proceedings	print	International	R&D	301-500	IBM
Sebastian Clauß: "Datenschutzgerechtes Identitätsmanagement", talk at "neue Verwaltung – 10. Kongress mit Fachmesse eGovernment", Forum H – "Datenschutz und Datensicherheit"	2009-05-05	talk	oral	National	government authorities	26-50	TUD
Interview with Marit Hansen, press publication "Twitter: Private Daten auf dem Präsentierteller"	2009-05-08	interview	print	National	general public		ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Kai Rannenberg: "Identity Management and Privacy Standardisation" at "2009 Information Security Standardization International Forum" by TC-260 China Information Security Standardization Technical Committee, Beijing, China	2009-05-08	talk	oral	International	Industry, policy makers, Government authorities, and Academics	101-300	GUF
V. Di Lecce, M. Calabrese, V. Piuri: "An ontology-based approach to human telepresence", in IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA 2009), Hong Kong, China, May 2009	2009-05-11	article in proceedings	print	International	R&D		UNIMI
V. Di Lecce, A. Amato, V. Piuri: "Data fusion for user presence identification", in IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA 2009), Hong Kong, China, May 2009	2009-05-11	article in proceedings	print	International	R&D		UNIMI
Jan Camenisch: "Privacy Enhancing Technologies, Privacy By Design", presented at Pyt med privatlivet – eller Privacy by Design, www.pytmedprivatlivet.dk, invited talk	2009-05-15	talk	oral	National	policy makers	26-50	IBM
C. Blundo, S. Cimato, S. De Capitani di Vimercati, A. De Santis, S. Foresti, S. Paraboschi, and P. Samarati, "Efficient Key Management for Enforcing Access Control in Outsourced Scenario", in proceedings of the 24th IFIP TC-11 International Information Security Conference (SEC 2009), Cyprus, Greece, May 2009	2009-05-18	article in proceedings	print	International	R&D		UNIMI, UNIBG
Sandra Steinbrecher, Stephan Groÿ, and Markus Meichau: "Jason: A scalable reputation system for the semantic web", in Proceedings of IFIP Sec 2009, IFIP International Information Security Conference: Security and Privacy in Dynamic Environments, May 2009	2009-05-20	talk	oral	International	R&D	26-50	TUD
Interview, press publication "Social Networks speichern gelöschte Fotos"	2009-05-23	interview	print	National	general public		ULD
Interview with Marit Hansen: press publication "Social Network Seiten – Hindernis beim Bewerbungsverfahren?"	2009-05-25	interview	print	National	general public		ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Rigo Wenning, Meeting with NEC to encourage further development of standardisation initiatives in PRIMCluster	2009-05-26	presentation	oral	Europe	EC project	1-5	W3C
Interview with Marit Hansen, press publication "British Telecom – Rückzug aus Spion-Werbesystem"	2009-06-06	interview	print	National	general public		ULD
Simone Fischer-Hübner: "Presenting a PrimeLife Overview", at the SWITS (Swedish IT-Security network) seminar in Karlskrona, Sweden	2009-06-08	presentation	oral	National	R&D	26-50	KAU
Hans Hedbom: "Presenting work on Transparency in PrimeLife", at the SWITS (Swedish IT security network) seminar in Karlskrona, Sweden	2009-06-08	presentation	oral	National	R&D	26-50	KAU
Rigo Wenning, Meeting with Nexof-RA to discuss standardisation together with GRID and cloud computing projects	2009-06-11	presentation	online	Europe	EC project	26-50	W3C
V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati: "Fragmentation design for efficient query execution over sensitive distributed databases" in proceedings of the 29th International Conference on Distributed Computing Systems (ICDCS 2009), Montreal, Quebec, Canada, June 2009	2009-06-22	article in proceedings	print	International	R&D		UNIMI, UNIBG
Stefan Berthold, Rainer Böhme: "Valuating Privacy with Option Pricing Theory", Workshop on the Economics of Information Security (WEIS 2009)	2009-06-25	article in proceedings	online	International	general public		TUD
Stefan Berthold, Rainer Böhme: "Valuating Privacy with Option Pricing Theory", Workshop on the Economics of Information Security (WEIS 2009)	2009-06-25	talk	oral	International	R&D	101-300	TUD
Rainer Böhme: "Position Statement to EU Security Economics Workshop", HP London	2009-06-26	talk	oral	International	government authorities	11-25	TUD
Stefanie Pötzsch, "Privacy Awareness: A Means to Solve the Privacy Paradox?", volume 298 of IFIP Advances in Information and Communication Technology, pp. 226-236. Springer, Boston, 2009	2009-07	article in proceedings	print	International	R&D		TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Hans Hedbom: "A Survey on Transparency Tools for Enhancing Privacy", in: The Future of Identity in the Information Society, Proceedings of the 4th IFIP/FIDIS Summer School, Brno, September 2008. published by Springer in July 2009	2009-07	article in proceedings	print	International	R&D	101-300	KAU
P. Samarati, "Protecting Information Privacy in the Electronic Society", in International Conference on Security and Cryptography (SECRYPT 2009), Milan, Italy, July 7-10, 2009	2009-07-07	keynote	oral	International	R&D		UNIMI
V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati: "Enforcing Confidentiality Constraints on Sensitive Databases with Lightweight Trusted Clients", in Proc. of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2009), Montreal, Quebec, Canada, July 2009	2009-07-12	article in proceedings	print	International	R&D		UNIMI, UNIBG
Interview with Marit Hansen, press publication "Datenschutz für Facebook-User unerwartet wichtig"	2009-07-14	interview	print	National	general public		ULD
Interview with Marit Hansen, press publication "Social-Network-Seiten sind wahre Fundgruben für Phisher"	2009-07-16	interview	print	National	general public		ULD
Simone Fischer-Hübner: "Technology and Identity Management", at International Hanse Roundtable on Privacy, Delmenhorst, Germany	2009-07-20	presentation	oral	International	R&D	26-50	KAU
Interview with Marit Hansen, press publication "Europäische Bankdaten bleiben im Visier der US-Fahnder"	2009-07-25	interview	print	National	general public		ULD
P. Samarati: "Privacy and Data Protection", in The European Intensive Programme on Information and Communication Security (IPICS 2009), Vienna, Austria	2009-07-27	talk	oral	International	R&D		UNIMI
Martin Pekárek, Stefanie Pötzsch: "A comparison of privacy issues in collaborative workspaces and social networks", in Identity in the Information Society, 2009, Special Issue on Social Web and Identity	2009-07-28	journal article	online	International	R&D		TUD, TILT
Simone Fischer-Hübner: "Presenting PrimeLife" at the IPICS Summer School at TU Vienna, Austria	2009-07-29	presentation	oral	International	R&D	51-100	KAU
F. Beato, M. Kohlweiss, K. Wouters: "Enforcing access control in social networks", HotPETs 2009, Seattle, WA, USA, 2009	2009-08-05 to 2009-08-07	conference session	print	International	R&D		KU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Stefan Schiffner, Sebastian Clauß: "Using Linkability Information to Attack Mix-based Anonymity Services", in: Proceedings of Privacy Enhancing Technologies 9th International Symposium, PETS 2009, Seattle, WA, USA, August 5-7, 2009, LNCS 5672, Springer, Berlin/Heidelberg, 2009, pp. 94-107	2009-08-05 to 2009-08-07	article in proceedings	print	International	R&D		TUD, KU
A. Rial, M. Kohlweiss, B. Preneel. "Universally composable adaptive priced oblivious transfer", in Pairing-Based Cryptography – Pairing 2009, Lecture Notes in Computer Science, p. 24, Palo Alto, CA, USA, Springer, 2009	2009-08-12 to 2009-08-14	article in proceedings	print	International	R&D		KU
Jan Camenisch: "Privacy Enhancing Cryptography: Theory and Practice", presented at Selected Areas of Cryptography, Calgary, Canada, invited talk	2009-08-13	talk	oral	International	R&D	101-300	IBM
Interview with Marit Hansen, press publication "Tatort Internet: Polizei will 2000 Cyber-Cops"	2009-08-14	interview	print	National	general public		ULD
M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, H. Shacham: "Randomizable proofs and delegatable anonymous credentials", talk held at Advances in Cryptology – CRYPTO 2009, Santa Barbara, CA, USA	2009-08-16 to 2009-08-20	talk	print	International	R&D	301-500	IBM, KU, UBR
Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, Hovav Shacham: "Proofs and Delegatable Anonymous Credentials", in Proceedings of CRYPTO 2009, pp. 108-125, Springer LNCS, 2009	2009-08-16 to 2009-08-20	article in proceedings	print	International	R&D	301-500	IBM
Benjamin Kellermann: "Privacy-Enhanced Event Scheduling", presentation at the PASSAT 2009, Vancouver, Canada	2009-08-29	talk	print	International	R&D	11-25	TUD
Benjamin Kellermann, Rainer Böhme: "Privacy-enhanced event scheduling", at IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT '09), 3:52-59, 2009	2009-08-29	article in proceedings	print	International	R&D		TUD
P. Samarati, "Privacy-Aware Data Management and Information Security", in Extending Database Technology school (EDBT school 2009), Presqu'île de Giens, France, August 30-September 4, 2009	2009-08-30	talk	oral	International	R&D		UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Simone Fischer-Hübner, Steven Furnell, Costas Lambrinouidakis: "Exploring Trust, Security and Privacy in Digital Business", Inauguration edition of the Journal: "Transactions on Large Scale Data and Knowledge Centered Systems", Vol.1, No.1, published by Springer Verlag within the LNCS journal subline 5729, September 2009	2009-09	journal article	print	International	R&D	301-500	KAU
Stephan Spitz: "Privacy on Mobile Devices: Present and Future Technologies", at eSmart conference, Sophia-Antipolis, France	2009-09	presentation	oral	International	industry	26-50	GD
Simone Fischer-Hübner, "Presenting PrimeLife at a panel" on "Is there a business case for privacy?" at the TrustBus 2009 conference in Linz, Austria	2009-09-03	presentation	oral	International	R&D	26-50	KAU
Fifth International Summer School organised jointly by the PrimeLife EU project in cooperation with the IFIP WG 9.2, 9.6/11.7 11.4, 11.6. Privacy and Identity Management for Life: "Privacy Tools"	2009-09-07 to 2009-09-11	workshop	oral	International	R&D, government authorities, industry, EC projects	51-100	KAU, SAP, all partners
Marc-Michael Bergfeld: "Privacy in Mobile Devices: Present and Future Technologies", keynote at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	keynote	oral	International	R&D, government authorities, industry, EC projects	51-100	GD
Ronald Leenes, Where the rubber meets the road: Privacy and Sociability in Social Network Sites, Fifth International Summer School organised jointly by the PrimeLife EU project in cooperation with the IFIP WG 9.2, 9.6/11.7 11.4, 11.6., Privacy and Identity Management for Life, Nice, France	2009-09-07 to 2009-09-11	keynote	oral	International	R&D, government authorities, industry, EC projects	51-100	TILT
S. De Capitani di Vimercati, "Privacy of Data", keynote at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	keynote	oral	International	R&D, government authorities, industry, EC projects	51-100	UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Jan Camenisch: "Privacy Enhancing Cryptography: Theory and Practice", keynote at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	keynote	oral	International	R&D, government authorities, industry, EC projects	51-100	IBM
Andreas Pfitzmann, "Lifelong Privacy", PrimeLife/IFIP WG 9.2, 9.6/11.7, 11.4, 11.6 Summer School "Privacy and Identity Management for Life", Nizza, September 8, 2009	2009-09-07 to 2009-09-11	keynote	oral	International	R&D, government authorities, industry, EC projects	51-100	TUD
Simone Fischer-Hübner, "Presenting PrimeLife HCI work" at the PrimeLife / IFIP Summer School in Nice	2009-09-07 to 2009-09-11	presentation	oral	International	R&D, government authorities, industry, EC projects	51-100	KAU
Hans Hedbom, "Presenting PrimeLife Transparency work" at the PrimeLife / IFIP Summer School in Nice ("Adding Secure Transparency Logging to the PRIME Core")	2009-09-07 to 2009-09-11	presentation	oral	International	R&D, government authorities, industry, EC projects	51-100	KAU
Stefanie Pöttsch and Katrin Borcea-Pfitzmann: "Privacy-Respecting Access Control in Collaborative Workspaces", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	oral	International	R&D, government authorities, industry, EC projects	51-100	TUD
Marit Hansen, Maren Raguse, Katalin Storf, Harald Zwingelberg: "Privacy from Womb to Tomb – Delegation from a European Perspective", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	print	International	R&D, government authorities, industry, EC projects	51-100	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Isabelle Oomen: "Out of Sight, Out of Mind?", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	oral	International	R&D, government authorities, industry, EC projects	51-100	TILT
André Deuker: "Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services" presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	print	International	R&D, government authorities, industry, EC projects	51-100	GUF
Hans Hedbom, Tobias Pulls, Peter Hjærtquist and Andreas Lavén: "Adding Secure Transparency Logging to the Prime Core", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	online	International	R&D, government authorities, industry, EC projects	51-100	KAU
Aleksandra Kuczerawy: "Facebook and its EU Users – Applicability of the EU Data Protection Law to US Based SNS", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	print	International	R&D, government authorities, industry, EC projects	51-100	KU
Erik Wästlund, Peter Wolkerstorfer: "PET-USES: The Privacy Enhancing Technology Users' Self-Estimation Scale", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	online	International	R&D, government authorities, industry, EC projects	51-100	KAU
Arnold Roosendaal: "Digital Personae and Profiles as Representations of Individuals", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	print	International	R&D, government authorities, industry, EC projects	51-100	TILT

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Benjamin Kellermann and Immanuel Scholz: "Anonymous Credentials in Web Applications – A Child's Play with the PRIME Core", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	oral	International	R&D, government authorities, industry, EC projects	51-100	TUD
Stefan Köpsell, Petr Švenda: "Secure logging of retained data – Combining smart cards, trusted timestamping servers and distributed storage", presentation at Fifth IFIP/PrimeLife Summer School, Nice, France, 2009	2009-09-07 to 2009-09-11	presentation	print	International	R&D, government authorities, industry, EC projects	51-100	TUD
Jan Camenisch: "A Crypto Toolbox to Build Your Own Protocols", at Information Security Conference, Pisa, Italy, keynote talk	2009-09-09	talk	oral	International	R&D	51-100	IBM
P. Samarati: "Protecting Data to Enable Privacy in the Electronic Society", in International Workshop on Signal Processing in the Encrypted Domain (SPEED 2009) Lausanne, Switzerland	2009-09-10	keynote	oral	International	R&D		UNIMI
Stefan Schiffner, Sebastian Clauß, Sandra Steinbrecher: "Privacy and Liveliness for Reputation Systems", 2009 European PKI Workshop (EuroPKI'09), Pisa, Italy	2009-09-11	talk	oral	International	R&D	26-50	TUD, KU
Simone Fischer-Hübner: presenting PrimeLife concepts at a panel at the Nordic Security Day, Oslo, Norway	2009-09-14	conference session	oral	International	R&D	51-100	KAU
Simone Fischer-Hübner: "presenting PrimeLife within a presentation on 'Gläserner Mensch?'" – Digitale Forensik: Spannungsfeld zwischen Strafverfolgung und Privatsphäre", B9	2009-09-16	keynote	oral	National	R&D	51-100	KAU
V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati: "Keep a Few: Outsourcing Data While Maintaining Confidentiality", in proceedings of the 14th European Symposium On Research, in: Computer Security (ESORICS 2009), Saint Malo, France	2009-09-21	article in proceedings	print	International	R&D		UNIMI, UNIBG

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Anssi Hoikkanen, Wainer Lusoli, Ioannis Maghiros, Ramón Compañó, Margherita Bacigalupo, Ian Brown, Jos Dumortier, Gloria González Fuster, Marit Hansen, Ronald Leenes, Yves Pouillet, Giovanni Sartor, Thilo Weichert: "White Paper on Regulatory and Legal Aspects of eIdentity"	2009-09-21	brochure	print	international	R&D, industry, government		ULD, TILT
Rigo Wenning, Open Digital Rights Workshop, Nancy, France	2009-09-21	workshop	online	International	R&D	11-25	W3C
Simone Fischer-Hübner: "Usable Privacy & Security", seminar on Security & Usability, organised by the company Todos, Göteborg, Sweden	2009-09-22	keynote	oral	International	industry	26-50	KAU
Kai Rannenberg: "Privacy in a world of ambient and personalized ICT Services", at "The Net will not forget", European conference on ICT and Privacy, Copenhagen, Denmark	2009-09-23	talk	print	International	general public	101-300	GUF
Meeting of Sascha Koschinat, Christian Weber, Gökhan Bal with Michael Marhöfer from Nokia Siemens Networks on PrimeLife's research directions and possible co-operation with a project about IdM & Privacy Enablers of Communication Service Providers	2009-09-24	talk	oral	Europe	industry	1-5	GUF
Simone Fischer-Hübner: "Usable Privacy and Identity Management – Challenges for the Future", at NordSec 2009, Oslo, Norway	2009-09-25	keynote	oral	International	R&D	51-100	KAU
Marit Hansen: "Spuren im Netz – der Schutz der Privatsphäre", Talk at the ISG Conference in Erfurt, Germany	2009-09-26	presentation	oral	National	general public	26-50	ULD
Marit Hansen: "Putting Privacy Pictograms into Practice – A European Perspective", in Stefan Fischer, Erik Maehle, Rüdiger Reischuk (eds.): "INFORMATIK 2009 – Im Focus das Leben", LNI P-154, Gesellschaft für Informatik, Bonn 2009, Workshop "Sicherer Umgang mit sensiblen Daten – technische Prävention und Reaktionen auf Datenschutzverletzungen"	2009-09-28	article in proceedings	print	National	R&D		ULD
Marit Hansen: "Putting Privacy Pictograms into Practice – A European Perspective", presentation at INFORMATIK 2009, Workshop "Sicherer Umgang mit sensiblen Daten – technische Prävention und Reaktionen auf Datenschutzverletzungen", Lübeck, Germany	2009-09-28	presentation	oral	National	R&D		ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Interview with Marit Hansen, press publication "Die Kriminalpolizei rät 3&4, Leitartikel", pressto gmbh – agentur für medienkommunikation. Published as "Anonymität ist verführerisch" in "Die Kriminalpolizei rät ..." 2009, pp. 22-28	2009-10	interview	print	National	general public		ULD
Stefanie Pötzsch: "Untersuchung des Einfusses von wahrgenommener Privatsphäre und Anonymität auf die Kommunikation in einer Online-Community", in S. Fischer, E. Maehle, and R. Reischuk (eds.): Informatik 2009, Im Fokus das Leben, 28 September-02 October 2009,Lübeck, volume 154 of Lecture Notes in Informatics, pp. 2152-2165, Bonn, 2009, Gesellschaft für Informatik	2009-10-02	article in proceedings	print	National	R&D		TUD
Benjamin Kellermann: "Datenschutzfreundliche Terminplanung", presentation at the Datenspuren 2009, Dresden, Germany	2009-10-03	presentation	online	National	general public	26-50	TUD
Gregory Neven: "PrimeLife Policy Language: Privacy-enhancing and credential-based extensions to XACML and SAML", at 2nd PRIMCluster Workshop, Brussels, Belgium, 2009	2009-10-06	presentation	oral	International	standardisation body	11-25	IBM
PRIMCluster meeting #2: PrimeLife, SWIFT, TAS3, Discussion on common interests in the areas of policies, preparation for the upcoming standardisation workshop in Luxembourg in November	2009-10-06	talk	oral	Europe	EC project	11-25	IBM, UNIMI, SAP
FIA Preparation meeting: Contribution to the discussions in the direction of PrimeLife thinking for stronger privacy protection	2009-10-07	talk	oral	Europe	policy makers	26-50	IBM
Simone Fischer-Hübner, "presenting PrimeLife" at a PhD course at Karlstad University	2009-10-12	presentation	oral	National	R&D	26-50	KAU
Isabelle Oomen, Lecture about privacy and social network sites at the University of Amsterdam for master students Philosophy	2009-10-12	talk	oral	National	general public	11-25	TILT
Ronald Leenes: "Identiteitsmanagement", juridische dag SURF-IBO, Utrecht	2009-10-13	talk	oral	national	R&D	30	TILT
Erik Wästlund "User Innovation: Consumer Needs and Wishes" at E-Clic Entrepreneurship Week at the University of Stavanger, Norway	2009-10-13	presentation	oral	International	EC project	11-25	KAU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Sebastian Clauß, Marit Hansen, Andreas Pfitzmann, Maren Raguse, Sandra Steinbrecher: "Tackling the Challenge of Lifelong Privacy", eChallenges e-2009 Conference Proceedings (Paul Cunningham, Miriam Cunningham (eds.)), IIMC Intern. Information Management Corporation, 2009	2009-10-22	talk	oral	International	R&D	26-50	ULD, TUD
Marit Hansen: "How to prevent data breaches", EDPS/ENISA Seminar "Responding to Data Breaches", October 23, 2009, Brussels, Belgium	2009-10-23	presentation	oral	Europe	policy makers	51-100	ULD
Katalin Storf, Jan Schallaböck: Third PrivacyOS Conference in co-location with the Austrian Big Brother Awards	2009-10-26 to 2009-10-27	conference session	oral	Europe	EC project	26-50	ULD
Simone Fischer-Hübner, Hans Hedbom: "Interview for Forskning & Framsteg", No. 7/2009, printed in article "Identitetskris på Nätet"	2009-11	interview	online	National	R&D		KAU
Stephan Spitz, Marc-Michael Bergfeld: "Creating Confidence in Mobile Services", article on privacy for mobile devices and the PrimeLife project in G&D's corporate publication "Smart" which is distributed to clients, partners and staff	2009-11	brochure	print	International	industry	>1000	GD
Rigo Wenning: "Privacy on the Web of Applications – Challenges and Opportunities", talk held at TPAC 2009, Santa Clara, California, USA	2009-11-02 to 2009-11-06	talk	oral	International	standardisation body	101-300	W3C
Ronald Leenes: "Where the rubber meets the road: Privacy and Sociability in Social Network Sites", workshop on future research challenges for privacy and security in online social networks, Leuven, Belgium	2009-11-05	talk	oral	Europe	R&D	60	TILT
Kai Rannenberg: "Privacy by Design – The role of Standardisation, Today is Tomorrow", Panel presentation at 31st International Conference of Data Protection and Privacy Commissioners, Madrid, Spain	2009-11-06	talk	oral	International	government authorities	301-500	GUF
P. Samarati: "Protecting Data Privacy in Outsourcing Scenarios", at Illinois Institute of Technology, Chicago, IL, USA	2009-11-11	keynote	oral	International	R&D		UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
C. A. Ardagna, S. De Capitani di Vimercati, S. Paraboschi, E. Pedrini, P. Samarati: "An XACML-based privacy-centered access control system", in proceedings of the 1st ACM Workshop on Information Security Governance (WISG 2009), Chicago, IL, USA	2009-11-13	article in proceedings	print	International	R&D		UNIMI, UNIBG
Katalin Storf: "Datenschutz in Social Networks und Online Spielen", Mediatage Nord, Kiel, Germany	2009-11-16	conference session	oral	National	general public	26-50	ULD
Marit Hansen: "Privacy-relevant features of current eID concepts in Germany", presentation at 4th adapID Workshop, Leuven, Belgium	2009-11-17	presentation	oral	International	R&D, government, industry, EC projects, standardisation	26-50	ULD
PrimeLife & W3C Workshop on Access Control Application Scenarios, Abbaye de Neumünster, Luxembourg, minutes and slides are available online: http://www.w3.org/2009/policy-ws/	2009-11-17 to 2009-11-18	workshop	online	International	R&D, government, industry, EC projects, standardisation	11-25	IBM, ULD, UNIMI, W3C, UNIBG, EMIC, SAP
Laurent Bussard, Moritz Y. Becker: "Can Access Control be Extended to Deal with Data Handling in Privacy Scenarios?", presentation at PrimeLife & W3C Workshop on Access Control Application Scenarios, Abbaye de Neumünster, Luxembourg	2009-11-17 to 2009-11-18	conference session	oral	International	R&D, government, industry, EC projects, standardisation	26-50	EMIC
Ulrich Pinsdorf, Jan Schallaboeck, Stuart Short: "Requirements for Policies in Cross-Domain Services Composition", presentation at PrimeLife & W3C Workshop on Access Control Application Scenarios, Abbaye de Neumünster, Luxembourg	2009-11-17 to 2009-11-18	conference session	oral	International	R&D, government, industry, EC projects, standardisation	26-50	ULD, EMIC, SAP
Bibi van den Berg, M.E. Pekárek: "SpotAFriendNow: Social interaction through location-based social networks", in Information, Communication and Society	2009-11-18	journal article	print	International	R&D	>1000	TILT

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Identity Management, Kolloquium "15 Jahre kommerzielles Internet in Dresden", IBH IT-Service GmbH, Dresden, Germany	2009-11-20	talk	oral	National	general public	26-50	TUD
Benjamin Kellermann: "Privacy-Enhanced Event Scheduling", Lightening Talk at the Metalab deepsec afterparty, Vienna, Austria	2009-11-20	presentation	oral	International	general public	26-50	TUD
Kai Rannenber: "Multilateral Security and Trust – the foundation for building the eUnion", EU 5th Ministerial eGovernment Conference, Malmö, Sweden	2009-11-20	talk	oral	Europe	government authorities	101-300	GUF
Slim Trabelsi, Vincent Salzgeber, Michele Bezzi, Gilles Montagnon: "Data Disclosure Risk Evaluation", at IEEE The International Conference on Risks and Security of Internet and Systems, CRISIS 2009	2009-11-22	conference session	oral	International	R&D	101-300	SAP
Simone Fischer-Hübner presenting PrimeLife at a panel at the Future Internet Assembly (FIA) in Stockholm, Sweden	2009-11-23	presentation	oral	International	EU Commission	51-100	KAU
Kai Rannenber: Session eID management and provisioning in the Future Internet infrastructures including routing, services, and content, Stockholm, Sweden	2009-11-23	talk	oral	Europe	R&D	51-100	GUF
Kai Rannenber: PrimeLife presentation at Session Identity management in Service Oriented Architectures, Stockholm, Sweden	2009-11-23	talk	oral	Europe	R&D	11-25	GUF
Slim Trabelsi: "Security and Privacy Research", at Ecole Nationale d'Ingenieurs de Tunis (ENIT)	2009-11-39	talk	oral	International	general public	51-100	SAP
Press coverage: PrimeLife was voted to be Project of the month by the NGO website Gov2u, http://www.gov2u.org/	2009-12	press coverage	online	International	general public	> 1000	3rd party
Maren Raguse: "Identitätsmanagement Privacy4Life", Lecture at University of Applied Science Kiel	2009-12-02	talk	oral	National	general public	11-25	ULD
Marc-Michael Bergfeld: "Privacy on Mobile Devices: Present and Future Technologies", at PrimeLife – STORK Workshop, IBM in Zürich, Switzerland	2009-12-10 to 2009-12-11	presentation	oral	International	EC project	11-25	GD
STORK/PrimeLife Workshop in Zurich	2009-12-10 to 2009-12-11	workshop	oral	Europe	R&D	11-25	IBM, TILT, W3C, KU, GD, EMIC

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Simone Fischer-Hübner: "Usable Privacy and Identity Management", Colloquium, Universität Mannheim, Germany	2009-12-11	presentation	oral	National	R&D	11-25	KAU
Simone Fischer-Hübner: "Usable Privacy and Identity Management", Colloquium, CASED/Frauenhofer & TU Darmstadt, Germany	2009-12-14	presentation	oral	National	R&D	11-25	KAU
Magali Seguran: "Security and Privacy Research", at Jean Moulin University Lyon	2009-12-15	talk	oral	National	general public	51-100	SAP
Benjamin Kellermann: "Privacy-Enhanced Event Scheduling", presentation at the 26C3, Berlin, Germany	2009-12-30	talk	online	International	general public	101-300	TUD
Benjamin Kellermann: "Datenschutzfreundliche terminplanung", in: Matthias Mehldau, (ed.) proceedings of the 26th Chaos Communication Congress	2009-12-30	article in proceedings	print	International	general public		TUD
Kai Rannenber, Several Teaching Lessons at GUF on PrimeLife related topics	2009- all over the year	presentation	oral	International	general public	101-300	GUF
Sandra Steinbrecher, Andreas Pfitzmann, Sebastian Clauß: "Identitätsmanagement in Netzwelten", in: Dieter Klumpp, Herbert Kubicek, Alexander Roßnagel, Wolfgang Schulz (eds.): Netzwelt – Wege, Werte, Wandel, Springer, Berlin Heidelberg 2010, pp. 245-263	2010-01	article in proceedings	print	National	general public		TUD
Simone Fischer-Hübner: "The Conflict between Privacy and Digital Forensics", 4.Band des Wiener Symposiums zum Wirtschafts- und Finanzstrafrecht, Wien, January 2010	2010-01	article in proceedings	print	Europe	policy makers	101-300	KAU
Simone Fischer-Hübner, "Hon är navet i svensk integritetsforskning", at Interview for Computer Sweden/IDG	2010-01-12	interview	print	National	industry	>1000	KAU
Marit Hansen, interview for the London Economics Study on PETs	2010-01-12	interview	oral	Europe	EU Commission		ULD
Harald Zwingelberg: "Identity Management in Social Networks", lecture at Wirtschaftsakademie Schleswig-Holstein, Kiel, Germany	2010-01-14	talk	oral	National	general public	26-50	ULD
Press coverage on PrimeLife Prototype "Cliques" in Nederlands Dagblad, two articles, one on the front page	2010-01-20	interview	print	National	general public	>1000	TILT
Kai Rannenber: "Privacy by Design in Mobile Applications & Location Based Services" at Privacy by Design: The Gold Standard, Toronto, Canada	2010-01-28	talk	oral	International	industry	101-300	GUF

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Kai Rannenberg: "On Privacy by Design" at MaRS Seminar Toronto, Canada	2010-01-29	talk	oral	International	R&D	11-25	GUF
Ernst-Jan Hamel : "Tilburg bouwt privacyvriendelijk sociaal netwerk", Interview with Bibi van den Berg on the release of PrimeLife's Social Network software Clique	2010-01-30	interview	online	National	general public	>1000	TILT
Press coverage on PrimeLife Prototype "Clique" at Nu.nl	2010-01-30	interview	online	National	general public	>1000	TILT
Membership in the "eID Survey Advisory Board" of the Institute for Prospective Technological Studies (IPTS), Seville, Spain	2010-02	membership	oral	National	privacy project	11-25	ULD
Radio coverage, Radio 1 interview on Lunch! about PrimeLife prototype "Clique"	2010-02-01	radio coverage	online	National	general public	>1000	TILT
Harald Zwingelberg: "Identity management and lifelong privacy", lecture at Wirtschaftsakademie Schleswig-Holstein, Kiel, Germany	2010-02-04	presentation	oral	National	general public	26-50	ULD
Marit Hansen, Holger Brocks: presentations at Safer Internet Day 2010, Ahrensburg, Germany	2010-02-09	presentation	oral	National	general public		ULD
Kai Rannenberg: session Intro and Chairing, Conference on Trust in the Info Society, León, Spain	2010-02-10 to 2010-02-11	conference session	oral	International	R&D	101-300	GUF
Interview with Marit Hansen on the service PleaseRobMe.com and general issues of online security	2010-02-18	interview	online	National	general public	>1000	ULD
Kai Rannenberg: ISO TMB/Privacy Steering Committee, Berlin, Germany	2010-02-24	presentation	oral	International	government authorities, industry	26-50	GUF
Participation in the Advisory Board of the project "Verbraucher sicher online" http://www.verbraucher-sicher-online.de/	2010-02-25	membership	online	National	general public	>1000	ULD
Interview with Marit Hansen on Social Networks with Bayerischer Rundfunk	2010-02-26	interview	online	National	general public	>1000	ULD
Stefanie Pöttsch, Katrin Borcea-Pfutzmann: "Privacy-Respecting Access Control in Collaborative Workspaces", in: Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, Ge Zhang: Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, Vol. 320, Springer Boston, 2010	2010	article in proceedings	print	International	R&D		TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Andreas Pfitzmann, Katrin Borcea-Pfitzmann: "Lifelong Privacy: Privacy and Identity Management for Life", In: Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, Ge Zhang: Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, Vol. 320, Springer Boston, 2010	2010	article in proceedings	print	International	R&D		TUD
Anja Lorenz, Katrin Borcea-Pfitzmann: "Role management in a privacy-enhanced collaborative environment", Interactive Technology and Smart Education, Vol. 7 Issue 2, pp.102-112, Emerald Group Publishing Limited, 2010	2010	journal article	print	International	R&D		TUD
Ronald Leenes: "Context is everything: sociality and privacy in Online Social Network Sites", in: Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, Ge Zhang: Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, Vol. 320, Springer, Boston 2010, pp. 48-65	2010	article in proceedings	print	International	general public	>1000	TILT
Jan Camenisch, Gregory Neven: "Saving on-line privacy", in: Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, Ge Zhang: Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, Vol. 320, Springer, Boston 2010, pp. 34-47	2010	article in proceedings	print	International	R&D		IBM
Hans Hedbom, Tobias Pulls, Peter Hjærtquist, Andreas Lavén: "Adding Secure Transparency Logging to the PRIME Core.Privacy and Identity Management for Life", 5th IFIP WG 9.2,9.6/11.7,11.4,11.6 / PrimeLife International Summer School, Nice, France, 2009, Revised Selected Papers, Springer 2010	2010	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	KAU
Erik Wästlund, Peter Wolkerstorfer, Christina Köffel: "PET-USES: Privacy-Enhancing Technology – Users' Self-Estimation Scale.Privacy and Identity Management for Life", 5th IFIP WG 9.2,9.6/11.7,11.4,11.6 / PrimeLife International Summer School, Nice, France, 2009, Revised Selected Papers, Springer 2010	2010	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	KAU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Elisabeth de Leeuw, Simone Fischer-Hübner, Lothar Fritsch (eds.): "Policies and Research in Identity Management", Proceedings of the 2nd IFIP WG11.6 working conference IDMAN 2010, Oslo, Norway, November 2010, Springer	2010	Proceedings	print	International	R&D	51-100	KAU
Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, Ge Zhang (eds.): "Privacy and Identity Management for Life", Proceedings of the 5th IFIP/PrimeLife International Summer School, Nice/France, September 7-11, 2009, revised selected papers, published by Springer in 2010	2010	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	101-300	KAU
Several Teaching Lessons at GUF	2010	presentation	oral	International	general public	101-300	GUF
Bibi van den Berg, Ronald Leenes, "Audience segregation in social network sites", in: Proceedings for SocialCom2010/PASSAT2010 (Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust), SocialCom2010/PASSAT2010 (Second IEEE International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust). Minneapolis (Minnesota, USA), Washington: IEEE, pp. 1111-1117	2010	article in proceedings	print	International	R&D	>1000	TILT
Simone Fischer-Hübner, John Sören Pettersson: "Usable Privacy-Enhancing Identity Management: Challenges and Approaches", in: Information and Communication Technologies, Society and Human Beings: Theory and Framework. Honouring Professor Gunilla Bradley, IGI Global, 2010	2010	article in proceedings	print	International	R&D	51-100	KAU
Simone Fischer-Hübner: "The Conflict between Privacy and Digital Forensics", in: Wirtschafts- und Finanzstrafrecht in der Praxis, Band 4, 2010, Linde Verlag	2010	article in proceedings	print	National	R&D	301-500	KAU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Sara Foresti, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, Mario Verdicchio: "Fine-grained disclosure of access policies", in M. Soriano, S. Qing, J. López, editors, 12th International Conference on Information and Communications Security – ICICS 2010, volume 6476 of Lecture Notes in Computer Science, pp. 16-30. Springer-Verlag, 2010	2010	article in proceedings	print	International	R&D		IBM, UNIBG, UNIMI
Patrik Bichsel, Jan Camenisch, Gregory Neven, Nigel P. Smart, Bogdan Warinschi: "Get Shorty via group signatures without encryption", In J. Garay and R. De Prisco, editors, 7th International Conference on Security and Cryptography for Networks – SCN 2010, volume 6280 of Lecture Notes in Computer Science, pp. 381-398. Springer-Verlag, 2010	2010	article in proceedings	print	International	R&D		IBM
Laurent Bussard, Gregory Neven, Franz-Stefan Preiss: "Downstream usage control", in IEEE International Symposium on Policies for Distributed Systems and Networks – POLICY 2010", pp. 22-29. IEEE Computer Society, 2010	2010	article in proceedings	print	International	R&D		EMIC, IBM
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, Mario Verdicchio: "Enabling privacy-preserving credential-based access control with XACML and SAML", in 10th IEEE International Conference on Computer and Information Technology – CIT 2010, pp. 1090-1095. IEEE Computer Society, 2010	2010	article in proceedings	print	International	R&D		IBM, UNIBG, UNIMI
Jan Camenisch, Sebastian Mödersheim, Gregory Neven, Franz-Stefan Preiss, Dieter Sommer: "A card requirements language enabling privacy-preserving access control", in J. Joshi and B. Carminati (eds.): 15th ACM Symposium on Access Control Models and Technologies – SACMAT 2010, pp. 119-128. ACM, 2010	2010	article in proceedings	print	International	R&D		IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Jan Camenisch, Maria Dubovitskaya, Gregory Neven: "Unlinkable priced oblivious transfer with rechargeable wallets", in R. Sion, editor, 14th International Conference on Financial Cryptography and Data Security – FC 2010, volume 6052 of Lecture Notes in Computer Science, pp. 66-81. Springer-Verlag, 2010	2010	article in proceedings	print	International	R&D		IBM
Michel Abdalla, Mihir Bellare, Gregory Neven: "Robust encryption", in D. Micciancio (ed.): 7th Theory of Cryptography Conference – TCC 2010, volume 5978 of Lecture Notes in Computer Science, pp. 480-497. Springer-Verlag, 2010	2010	article in proceedings	print	International	R&D		IBM
Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, Mario Verdicchio: "Exploiting cryptography for privacy-enhanced access control", Journal of Computer Security 18(1), pp. 123-160, 2010	2010	article in proceedings	print	International	R&D		IBM
Jan Camenisch, Nathalie Casati, Thomas Groß, Victor Shoup: "Credential Authenticated Identification and Key Exchange", CRYPTO 2010, pp. 255-276	2010	article in proceedings	print	International	R&D	301-500	IBM
Jan Camenisch, Sebastian Mödersheim, Dieter Sommer: "A Formal Model of Identity Mixer", FMICS 2010, pp. 198-214	2010	article in proceedings	print	International	R&D	51-100	IBM
Jan Camenisch, Maria Dubovitskaya, Gregory Neven: "Unlinkable Priced Oblivious Transfer with Rechargeable Wallets", Financial Cryptography 2010, pp. 66-81	2010	article in proceedings	print	International	R&D	51-100	IBM
Jan Camenisch, Markulf Kohlweiss, Claudio Soriente: "Solving Revocation with Efficient Update of Anonymous Credentials", SCN 2010, pp. 454-471	2010	article in proceedings	print	International	R&D	101-300	IBM
Jan Camenisch: "Privacy-Enhancing Cryptography: From Theory into Practice"	2010	article in proceedings	print	International	R&D	301-500	IBM
Endre Bangerter, Jan Camenisch, Stephan Krenn: "Efficiency Limitations for Σ -Protocols for Group Homomorphisms", TCC 2010, pp. 553-571	2010	article in proceedings	print	International	R&D	301-500	IBM
Christian Cachin, Jan Camenisch: "Encrypting Keys Securely", IEEE Security & Privacy 8(4): 66-69 (2010)	2010	article in proceedings	print	International	R&D	301-500	IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Michel Abdalla, Mihir Bellare, Gregory Neven, "Robust Encryption", to appear at TCC 2010	2010	article in proceedings	print	International	R&D	101-300	IBM
Marit Hansen: "Privacy 2.0 – Ein Reality-Check//Datenschutz im Web 2.0 – ein Auslaufmodell?", to be published in: Proceedings of "IT-Sicherheit am Donaustrand III", Symposium zu "Sicherheitstechnische und sicherheitsrechtliche Herausforderungen des Web 2.0" am Institut für IT-Sicherheit und Sicherheitsrecht (ISL) der Universität Passau at 16 February, 2009	2010-XX to appear	article in proceedings	print	National	R&D		ULD
Jan Camenisch, Javier Lopez, Fabio Massacci, Massimo Ciscato, Thomas Skordas: "JCS special issue on EU-funded ICT research on Trust and Security"	2010	journal article	print	International	R&D	301-500	IBM
J. Lapon, M. Kohlweiss, B. De Decker, V. Naessens: "Performance Analysis of Accumulator-based Revocation Mechanisms", in Proceedings of the 25th International Conference on Information Security (SEC 2010), IFIP Conference Proceedings, Kluwer, 12 pages, 2010	2010	article in proceedings	print	International	R&D		KU
Cornelia Graf, Peter Wolkerstorfer, Katrin Kristjansdottir, Manfred Tscheligi: "What is your privacy preference? An insight into Users understanding of Privacy Terms"	2010	interview	oral	International	general public	11-25	CURE
Cornelia Graf, Peter Wolkerstorfer, Arjan Geven, Manfred Tscheligi: "A Pattern Collection for Privacy Enhancing Technology"	2010	article in proceedings	online	International	general public	>1000	CURE
Stefan Schiffner, Sebastian Clauß, Sandra Steinbrecher: "Privacy and Liveliness for Reputation Systems", Lecture Notes in Computer Science, 2010, Volume 6391/2010, Springer-Verlag, p. 209-224	2010	article in proceedings	print	International	R&D	101-300	TUD
Sabrina De Capitani di Vimercati, S. Foresti, Pierangela Samarati: "Protecting Information Privacy in the Electronic Society", in e-Business and Telecommunications International Conference (ICETE 2009), Revised Selected Papers, J. Filipe, and M.S. Obaidat (eds.), Springer-Verlag, 2010	2010		print	International	R&D		UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Jan Camenisch, S. Moedersheim, Gregory Neven, Franz-Stefan. Preiss, Dieter Sommer: "A Card Requirements Language Enabling Privacy-Preserving Access Control", Proc. Of 15th ACM Symposium on Access Control Models and Technologies "SACMAT 2010", Pittsburg, PA (ACM New York, June 2010), pp. 119-128	2010	article in proceedings	print	International	R&D	301-500	IBM
Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, Mario Verdicchio: "Enabling Privacy-preserving Credential-based Access Control with XACML and SAML", Proc. of IEEE International Symposium on Trust, Security and Privacy for Emerging Applications 2010 (TSP-10), Bradford, UK	2010	article in proceedings	print	International	R&D	301-500	IBM, UNMI, UNIBG
Laurent Bussard, Gregory Neven, Franz-Stefan Preiss: "Downstream Usage Control", in proceedings of IEEE Policy 2010, July 2010	2010	article in proceedings	print	International	R&D	301-500	IBM
Simone Fischer-Hübner: Invited talk at SIG Security Annual meeting, 27. April, Stockholm	2010-01-27	keynote	oral	National	R&D	26-50	KAU
Jan Camenisch: "TCC 2010", Zurich, Privacy-Enhancing Cryptography: From Theory into Practice	2010-02-10	talk	oral	International	R&D	301-500	IBM
Jan Camenisch: "Trust in the Information Society", Leon, Spain. eID needs Privacy On	2010-02-11	talk		Europe	R&D		IBM
Simone Fischer-Hübner: Invited lecture at ISSA web conference, February 16, 2010	2010-02-16	presentation	oral	International	R&D	301-500	KAU
Anja Lorenz, Katrin Borcea-Pfutzmann: "Role management in a privacy-enhanced collaborative environment", in: Piet Kommers, Pedro Isafas: Proceedings of e-Society, IADIS, 2010	2010-03	article in proceedings	print	International	R&D		TUD,
Rainer Böhme, Stefanie Pötzsch: "Privacy in Online Social Lending", in Proceedings of the AAAI 2010 Spring Symposium on Intelligent Information Privacy Management, Palo Alto, California, pp. 23-28	2010-03	article in proceedings	online	International	R&D		TUD,

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Simone Fischer-Hübner, Marit Hansen, Hans Hedbom: "Technik für mehr Transparenz", in: digma – Zeitschrift für Datenrecht und Informationssicherheit 1/2010, Schulthess Verlag, March 2010, pp. 34-37	2010-03	journal article	print	National	R&D, industry, general public, governmental authorities, policy makers	>1000	KAU, ULD
Simone Fischer-Hübner, Marit Hansen, Hans Hedbom: "Technik für mehr Transparenz", in: digma – Zeitschrift für Datenrecht und Informationssicherheit 1/2010, Schulthess Verlag, March 2010, pp. 34-37	2010-03	journal article	print	National	R&D, industry, general public, governmental authorities, policy makers	>1000	KAU, ULD
Harald Zwingelberg, Ulrich König: "Selbstbestimmter Datenschutz: Lösungen für mehr Transparenz in Webshops und E-Mail", presentation at CeBIT, Heiseforum, Hanover, Germany	2010-03-03	presentation	oral	Europe	R&D, industry, general public	26-50	ULD
Sandra Steinbrecher: "The need for Interoperable Reputation Systems", iNetSec 2010: Open Research Problems in Network Security, Sofia, Bulgaria	2010-03-05 to 2010-03-06	talk	oral	International	R&D	11-25	TUD
Anja Lorenz, Katrin Borcea-Pfitzmann: "Role management in a privacy-enhanced collaborative environment"	2010-03-18	presentation	oral	International	R&D	26-50	TUD,
ULD: Contributions to: "Konferenz der Datenschutzbeauftragten des Bundes und der Länder: "Ein modernes Datenschutzrecht für das 21. Jahrhundert – Eckpunkte", March 18, 2010, http://www.lfd.mv.de/dschutz/beschlue/Eckpunkte.pdf .	2010-03-18	brochure	print	National	policy makers, journalists	>1000	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Pierangela Samarati: "Protecting Data Privacy in Outsourcing Scenarios," in 3rd International Workshop on Privacy and Anonymity in the Information Society (PAIS 2010), Lausanne, Switzerland, March 22, 2010	2010-03-22	keynote	oral	International	R&D	26-50	UNIMI
Rainer Böhme, Stefanie Pötzsch: "Privacy in Online Social Lending", AAAI 2010 Spring Symposium on Intelligent Information Privacy Management, Stanford University, California	2010-03-22 to 2010-03-24	presentation	oral	International	R&D	101-300	TUD,
Chapters "8.2 PrimeLife – Identitätsmanagement im Fokus" and "2.3.2 Internationale Standardisierung", in: 32. Tätigkeitsbericht des ULD (2010), Landtagsdrucksache 17/210, https://www.datenschutzzentrum.de/material/tb/tb32/	2010-03-23	brochure	print	National	policy makers, general public, governmental authorities, industry, journalists	>1000	ULD
Kai Rannenber: "Identity Assurance – Who gets the assurance, who carries the risk?" Keynote at RISE Workshop "Ethical and Policy Implications of Global Mobility and Security"	2010-03-25 to 2010-03-26	article in proceedings	online	International	R&D, policy makers, government authorities, industry, EC project	>1000	GUF
Sabrina De Capitani di Vimercati, S. Foresti, S. Jajodia, Stefano Paraboschi, Pierangela Samarati: "Encryption Policies for Regulating Access to Outsourced Data", in ACM Transactions on Database Systems (TODS), April, 2010	2010-04	journal article	print	International	R&D	>1000	UNIMI,UNIBG
Pierangela Samarati, Sabrina De Capitani di Vimercati: "Data Protection in Outsourcing Scenarios: Issues and Directions", in Proc. of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010), Beijing, China, April, 2010	2010-04	article in proceedings	print	International	R&D	101-300	UNIMI
Simone Fischer-Hübner: Interview in: Aktuell Sakerhet, No. 4, 2010	2010-04	interview	print	National	R&D	>1000	KAU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Marit Hansen: participation in the Dagstuhl Seminar 10141 "Distributed Usage Control", Dagstuhl, Germany	2010-04-06 to 2010-04-09	conference session	oral	International	R&D	26-50	ULD
Ronald Leenes: "Clique in 15 minutes"	2010-04-07	talk	oral	International	general public	101-300	TILT
Danah Boyd: "How Social Media is Reworking Privacy and Publicity"	2010-04-07	keynote	oral	International	general public	101-300	TILT
Andreas Pfitzmann, Marit Hansen: "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", Working Paper v0.33, April 08, 2010, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.pdf .	2010-04-08	brochure	online	International	R&D	>1000	TUD, ULD
Pierangela Samarati: "Data Protection in Outsourcing Scenarios: Issues and Directions," in 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010), Beijing, China, April 13-16, 2010	2010-04-13 to 2010-04-16	keynote	oral	International	R&D	101-300	UNIMI
Simone Fischer-Hübner: Invited talk at ISACA Scandinavian Conference, April 20, Gothenburg	2010-04-20	keynote	oral	International	R&D	101-300	KAU
Pierangela Samarati: "Data Protection in Outsourcing Scenarios," in MSc programme on Technoeconomic Management and Security of Digital Systems, University of Piraeus, Greece, April 23, 2010	2010-04-23	talk	oral	International	R&D	26-50	UNIMI
Katrin Borcea-Pfitzmann: "PrimeLife – Bringing sustainable privacy and identity management to future networks and services", GI-Jahrestagung, Frauen und Informatik, Dortmund	2010-04-24	talk	oral	National	general public	26-50	TUD
Marit Hansen: participation in the panel discussion "Web 2.0: Dein öffentliches Privatleben", University of Applied Sciences, Kiel, Germany	2010-04-29	conference session	oral	National	general public	101-300	ULD
C. Ardagna, Sabrina De Capitani di Vimercati, Stefano Paraboschi, E. Pedrini, P. Samarati, M. Verdicchio: "Expressive and Deployable Access Control in Open Web Service Applications", in IEEE Transactions on Service Computing (TSC), May, 2010	2010-05	journal article	print	International	R&D	>1000	UNIMI, UNI BG

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Marit Hansen, Sven Thomsen: "Lebenslanger Datenschutz – Anforderungen an vertrauenswürdige Infrastrukturen", in: Datenschutz und Datensicherheit (DuD) 34 (2010) 5, pp. 283-288	2010-05	journal article	print	National	policy makers, industry, governmental authorities, general public	>1000	ULD
Hans Hedbom, Tobias Pulls: "Unlinking Database Entries: Implementation Issues in Privacy Preserving Secure Logging", Proceedings of 2nd International Workshop on Security and Communication Networks , 2010, IEEE Xplore	2010-05	article in proceedings	print	International	R&D	>1000	KAU
Marit Hansen: "Datenschutz und Technik III – Datenschutzfördernde Technik", lecture at University of Kiel, Germany	2010-05-12	presentation	oral	National	general public	11-25	ULD
Gregory Neven: "How to win back privacy", Invited talk at Workshop on Digital Identity, Trust & Confidence, Swiss Academy of Engineering Sciences, May 20/21, 2010, Parkhotel Schloss Münchenwiler, Switzerland	2010-05-20	keynote	oral	National	government authorities	26-50	IBM
Simone Fischer-Hübner: Invited talk at ceremony of the Swedish Armed Forces (FM) with Swedish Universities, 21 May, Enköping	2010-05-21	keynote	oral	National	R&D	51-100	KAU
Gregory Neven: "The road to post-quantum privacy", Invited talk at Third International Workshop on Post-Quantum Cryptography, Darmstadt, Germany, May 25-28, 2010	2010-05-25	keynote	oral	International	R&D	51-100	IBM
Stefanie Pötzsch. "Feeling anonymous today? – An empirical study of the effect of privacy-awareness information on forum users", Poster presentation at General Online Research 10, Pforzheim	2010-05-26 to 2010-05-28	presentation	oral	International	R&D	101-300	TUD
Sandra Steinbrecher: "Interoperable and Secure Reputation Systems", Information Security Summit	2010-05-27	talk	oral	International	industry	51-100	TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Marit Hansen, Maren Raguse, Katalin Storf, Harald Zwingelberg: "Delegation for Privacy Management from Womb to Tomb – A European Perspective", in: Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, Ge Zhang (eds.): Privacy and Identity Management for Life, 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7-11, 2009, Revised Selected Papers, IFIP AICT 320, Springer, Berlin, Heidelberg, New York 2010, pp. 18-33	2010-06	article in proceedings	print	International	R&D, industry, policy makers	>1000	ULD
Marit Hansen: Spuren im Netz – der Schutz der Privatsphäre, in: Dieter Korczak (ed.): Spurensuche – Kulturwissenschaftliche Interpretationen und gesellschaftliche Rezeption, Tagungsband zur 66. Jahrestagung, Asanger-Verlag, Kröning 2010, pp. 105-128	2010-06	article in proceedings	print	National	policy makers, general public	500-1000	ULD
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, and Mario Verdicchio: "Enabling Privacy-Preserving Credential-Based Access Control with XACML and SAML", in Proc. of the 3rd IEEE International Symposium on Trust, Security and Privacy for Emerging Applications (TSP 2010), Bradford, UK, June-July, 2010	2010-06 to 2010-07	article in proceedings	print	International	R&D	101-300	IBM, UNIBG, UNIMI
Kai Rannenber: "Privacy by Design – Auf dem Weg zu einem effizienteren Datenschutz" Reimers-Kolleg, Bad Homburg	2010-06-02	keynote	oral	National	general public	51-100	GUF
Jan Camenisch: "First European Summit on the Future Internet", Luxembourg, Security and the Smarter Planet	2010-06-03	talk		Europe	EU Commission		IBM
Simone Fischer-Hübner: Presentation at the SWITS Seminar in Stockholm, June 7-8, 2010	2010-06-07	talk	oral	National	R&D	51-100	KAU
Hans Hedbom: Presentation at the SWITS Seminar in Stockholm, June 7-8, 2010	2010-06-07	talk	oral	National	R&D	51-100	KAU
Slim Trabelsi, Eric Weil, Alessandro Sorniotti, Stuart Short and Michele Bezzi "Privacy-Aware Policy Matching", IEEE symposium on Computers and Communications 2010, June 2010	2010-06-10	article in proceedings	online	International	R&D	>1000	SAP

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Slim Trabelsi, "Privacy-Aware Policy Matching", IEEE symposium on Computers and Communications 2010	2010-06-10	talk	oral	International	R&D, industry	>1000	SAP
Simone Fischer-Hübner, Hans Hedbom: Interview in Forskning&Framsteg, "Integritetskris på nätet", June 1, 2010	2010-06-10	interview	print	National	general public	>1000	KAU
Franz-Stefan Preiss: "Privacy-Preserving Access Control and A Credential Requirements Language Enabling It", SACMAT 2010", Pittsburgh, PA	2010-06-10	talk	oral	International	R&D	51-100	IBM
Simone Fischer-Hübner: Teaching PET course at FH Hagenberg, June 14-15, Hagenberg/Austria	2010-06-14	talk	oral	National	R&D	11-25	KAU
Kai Rannenber: "Privacy in mobile applications and beyond", Journée ADREAM, Architectures dynamiques reconfigurables pour systèmes embarqués autonomes mobiles, LAAS CNRS, Toulouse, France	2010-06-15	presentation	oral	International	industry, general public, R&D	101-300	GUF
Kai Rannenber: "Privacy in mobile applications and beyond", Journée ADREAM, Architectures dynamiques reconfigurables pour systèmes embarqués autonomes mobiles, LAAS CNRS, Toulouse, France	2010-06-15	article in proceedings	online	International	industry, general public, R&D	>1000	GUF
Marit Hansen, Harald Zwingelberg: Workshop on Ambient Assisted Living, together with the SmartAssist project, Kiel, Germany	2010-06-16	conference session	oral	National	EC project	6-10	ULD
Ronald Leenes: "Sociale netwerken die voldoen aan normen"	2010-06-17	keynote	oral	National	general public	101-300	TILT
Sandra Steinbrecher: "Online Privacy and Identity Management", Salon im Kunsthof, Dresden	2010-06-21	talk	oral	National	general public	11-25	TUD
Jan Camenisch: "Trust 2010", Berlin & Anonymous Signatures	2010-06-21	talk		International	R&D		IBM
Stefanie Pöttsch and Rainer Böhme: "The Role of Soft Information in Trust Building: Evidence from Online Social Lending", TRUST 2010, Berlin	2010-06-21 to 2010-06-23	presentation	oral	International	R&D	301-500	TUD
Panel on "Assured Information Sharing: Techniques and Challenges" at DBSec 2010 in Rome, Italy	2010-06-22	talk	oral	International	R&D	26-50	UNIBG
Katrin Borcea-Pfitzmann: Presenting the research field "Privacy by design" of chair DuD of Technische Universität Dresden @ Info Event of National Contact Point Security Research, Bonn	2010-06-24	presentation	oral	National	R&D, industry	101-300	TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Stefan Köpsell: Presenting the research fields "Anonymous Communication" and "Multimedia Forensics of chair DuD of Technische Universität Dresden @ Info Event of National Contact Point Security Research, Bonn	2010-06-24	presentation	oral	National	R&D, industry	101-300	TUD
Sabrina De Capitani di Vimercati, S. Foresti, S. Jajodia, Stefano Paraboschi, G. Pelosi, Pierangela Samarati: "Encryption-based Policy Enforcement for Cloud Storage", in Proc. of the 1st ICDCS Workshop on Security and Privacy in Cloud Computing (SPCC 2010), Genova, Italy, June 25, 2010	2010-06-25	article in proceedings	print	International	R&D	26-50	UNIMI,UNI BG
Pierangela Samarati: "Protecting Confidentiality in External Data Storage," in 1st International Workshop on Security and Privacy in Cloud Computing (SPCC 2010), Genoa, Italy, June 25, 2010	2010-06-25	keynote	oral	International	R&D	26-50	UNIMI
Sabrina De Capitani di Vimercati: "New Research Directions of Security and Privacy in Cloud Computing", in 1st International Workshop on Security and Privacy in Cloud Computing (SPCC 2010) Genoa, Italy June 25, 2010	2010-06-25	presentation	oral	International	R&D	26-50	UNIMI
C. Blundo, S. Cimato, Sabrina De Capitani di Vimercati, A. De Santis, S. Foresti, Stefano Paraboschi, Pierangela Samarati: "Managing Key Hierarchies for Access Control Enforcement: Heuristic Approaches", in Computers & Security, July, 2010	2010-07	journal article	print	International	R&D	>1000	UNIMI,UNI BG
V. Ciriani, Sabrina De Capitani di Vimercati, S. Foresti, S. Jajodia, Stefano Paraboschi, Pierangela Samarati: "Combining Fragmentation and Encryption to Protect Privacy in Data Storage", in ACM Transactions on Information and System Security (TISSEC), July, 2010	2010-07	journal article	print	International	R&D	>1000	UNIMI,UNI BG
Pierangela Samarati: "The European Intensive Programme on Information and Comm. Security (IPICS 2010)", Greece, 2010	2010-07	presentation	oral	Europe	general public	51-100	UNIMI
Laurent Bussard, Gregory Neven, Franz-Stefan Preiss: "Downstream Usage Control", in proceedings of IEEE Policy 2010, July 2010	2010-07	article in proceedings	print	International	R&D	26-50	EMIC / IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Leif-Erik Holtz: "Datenschutzkonformes Social Networking: Clique und Scramble!", in: Datenschutz und Datensicherheit 34 (2010) 7, pp. 439-443	2010-07	journal article	print	National	policy makers, industry, governmental authorities, general public	>1000	ULD
Franz-Stefan Preiss: "Privacy-Preserving Credential-Based Access Control and How to Enable It with XACML and SAML", IEEE International Symposium on Trust, Security and Privacy for Emerging Applications 2010 (TSP-10), Bradford, UK	2010-07-01	talk	oral	International	R&D		IBM
Thilo Weichert, Marit Hansen: "Schülerzeitungswettbewerb, Sonderpreis Datenschutz", Jury participation, Kiel, Germany	2010-07-08	conference session	print+oral	National	journalists, pupils	51-100	ULD
Ioannis Krontiris: "W3C Geolocation API calls for Better User Privacy Protection" at W3C Workshop on Privacy for Advanced Web APIs, London, UK	2010-07-12 to 2010-07-13	presentation	oral	International	standardisation body, R&D, industry	51-100	GUF
Ioannis Krontiris, Andreas Albers and Kai Rannenberg: "W3C Geolocation API calls for Better User Privacy Protection" at W3C Workshop on Privacy for Advanced Web APIs, London, UK	2010-07-12 to 2010-07-13	article in proceedings	online	International	standardisation body, R&D, industry	>1000	GUF
Hans Hedbom: Lectures at IPICS 2010 Summerschool in Samos	2010-07-19	talk	oral	International	R&D	51-60	KAU
Gregory Neven: "The PrimeLife Policy Language", Presentation at Workshop on Privacy in Intelligent Transportation Systems, July 20, 2010, Berlin, Germany	2010-07-20	talk	oral	International	R&D	26-50	IBM
Ulrich König: "Icons für E-Mail-Privacy"	2010-07-26	interview	online	National	journalists	>1000	ULD
Ulrich König: "Icons für E-Mail-Privacy" in IETF 78 Applications Area Open Meeting	2010-07-26	presentation	oral	International	standardisation body	51-100	ULD
Franz-Stefan Preiss: "Downstream Usage Control.", IEEE Policy 2010	2010-07-30	talk	oral	International	R&D	51-100	IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Stefanie Pöttsch, Rainer Böhme: "The Role of Soft Information in Trust Building: Evidence from Online Social Lending", in A. Acquisti, S.W. Smith, and A.-R. Sadeghi (eds.): TRUST 2010, LNCS 6101, pp. 381-395, Springer, Heidelberg, 2010	2010-08	article in proceedings	print	International	R&D		TUD
Jan Camenisch: "Privacy and Identity Management – Cryptographic Challenges", keynote held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02	keynote	oral	International	R&D, government authorities, EC project, policy makers	51-100	IBM
Andreas Pfitzmann: "Lifelong Privacy", keynote held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02	keynote	oral	International	R&D, government authorities, EC project, policy makers	51-100	TUD
Manuela Berg, Katrin Borcea-Pfitzmann: "Implementability of the Identity Management Part in Pfitzmann/Hansen's Terminology for a Complex Digital World", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02	presentation	oral	International	R&D, industry, policy makers	26-50	TUD
Manuela Berg, Katrin Borcea-Pfitzmann: "Implementability of the Identity Management Part in Pfitzmann/Hansen's Terminology for a Complex Digital World", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D		TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Harald Zwingelberg: "Necessary processing of personal data – The need-to-know principle and processing data from the new German identity card", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02 to 2010-08-06	presentation	oral	International	R&D, industry, policy makers	51-100	ULD
Marit Hansen: Co-Chairing of the IFIP/PrimeLife Summer School and panel discussion "What's the meaning of lifelong privacy?", Helsingborg, Sweden	2010-08-02 to 2010-08-06	conference session	oral	International	R&D, industry, policy makers	51-100	ULD
Stefan Berthold: "Towards a Formal Language for Privacy Options", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	KAU
Bibi van den Berg: "The Uncanny Valley Everywhere? On Privacy Perception and Expectation Management", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	TILT
Bibi van den Berg: "The Uncanny Valley Everywhere? On Privacy Perception and Expectation Management", keynote held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02 to 2010-08-06	keynote	oral	International	R&D, industry, policy makers	51-100	TILT
Aleksandra Kuczerawy, Fanny Coudert: "Privacy Settings in Social Networking Sites: Is It Fair?", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	KU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Jaromir Dobias: "Privacy Effects of Web Bugs Amplified by Web 2.0", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	TUD
Ulrich König: "PrimeLife Checkout – A Privacy-Enabling e-Shopping User Interface", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	ULD
Hannes Federrath, Marit Hansen and Michael Waidner: "Andreas Pfitzmann 1958-2010: Pioneer of Technical Privacy Protection in the Information Society", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	ULD
Leif-Erik Holtz, Katharina Nocun, Marit Hansen: "Towards Displaying Privacy Information with Icons", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	TUD
Ulrich König: "PrimeLife Checkout – A Privacy-Enabling e-Shopping User Interface", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02 to 2010-08-06	presentation	oral	International	R&D, industry, policy makers	26-50	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Leif-Erik Holtz, Marit Hansen: "Towards Displaying Privacy Information with Icons", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02 to 2010-08-06	presentation	oral	International	R&D, industry, policy makers	26-50	ULD
Kai Rannenberg: "Towards an Economic Valuation of Telco-based Identity Management Enablers" keynote held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-02 to 2010-08-06	keynote	oral	International	R&D, industry	51-100	GUF
Christian Weber: "eScience and Shared Workspaces: Enabler for next generation research environment" in: preproceedings of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2010-08-02 to 2010-08-06	article in proceedings	online	International	R&D	>1000	GUF
Marit Hansen: Co-chairing of the IFIP/PrimeLife Summer School + panel discussion "What's the meaning of lifelong privacy?", Helsingborg, Sweden	2010-08-02 to 2010-08-06	conference session	oral	International	R&D, industry, policy makers	51-100	ULD
Marit Hansen (chair), Bibi van den Berg, Sonja Buchegger, Jan Camenisch, Timothy Edgar, Andreas Pfitzmann, Diane Whitehouse (panelists): "Panel Discussion: What is the meaning of Lifelong Privacy", panel held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-03	conference session	print	International	R&D, government authorities, EC project, policy makers	51-100	many
Simone Fischer-Hübner (chair), Panelists: Anna Lysanskaya, Gregory Neven, Andreas Pfitzmann, Bernd Stahl, Alma Whitten (panelists): "Panel discussion – Privacy Research Trends ", panel held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-03	conference session	print	International	R&D, government authorities, EC project, policy makers	51-100	many
Harald Zwingelberg: "Necessary processing of personal data – The need-to-know principle and processing data from the new German identity card", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-03	presentation	oral	International	R&D, industry, policy makers	51-100	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Aleksandra Kuczerawy: "Privacy Settings in Social Networking Sites: Is It Fair?", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-04	presentation	oral	International	R&D, industry, policy makers	51-100	KU
Jaromir Dobias: "Privacy Effects of Web Bugs Amplified by Web 2.0", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-04	presentation	oral	International	R&D, industry, policy makers	26-50	TUD
Christian Weber: "eScience and Shared Workspaces: Enabler for next generation research environment" presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-04	presentation	oral	International	R&D	51-100	GUF
Michael Marhoefer, Gökhan Bal: "Controlling the Flow of PII to Web 2.0 beyond current Identity Service Provisioning", presented by M. Marhoefer at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-04	presentation	oral	International	R&D	51-100	GUF
Gregory Neven: "Privacy Policies in PrimeLife", keynote held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-05	keynote	oral	International	R&D	51-100	IBM
Anna Lysyanskaya: "Privacy by Crypto", keynote held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-05	keynote	oral	International	R&D	51-100	UBR
Ulrich König: "Primelife Checkout" – a Privacy enabling user interface, presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-05	presentation	oral	International	R&D, industry, policy makers	51-100	ULD
Leif-Erik Holtz, Marit Hansen: "Displaying privacy information with icons", presentation held at 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden	2010-08-06	presentation	oral	International	R&D, industry, policy makers	51-100	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Andreas Pfitzmann, Marit Hansen: "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", Working Paper v0.34, August 10, 2010, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf .	2010-08-10	brochure	online	International	R&D	>1000	TUD, ULD
C.A. Ardagna, Sabrina De Capitani di Vimercati, S. Foresti, Stefano Paraboschi, Pierangela Samarati: "Minimizing Disclosure of Private Information in Credential-Based Interactions: A Graph-Based Approach", in Proc. of the 2nd IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT 2010), Minneapolis, Minnesota, USA, August 20-22, 2010	2010-08-20 to 2010-08-21	article in proceedings	print	International	R&D	101-300	UNIMI,UNI BG
Bibi van den Berg: "Audience segregation in social network sites"	2010-08-22	talk					
Marit Hansen: "Kontrollverluste durch Informationstechnik", presentation at Sommerakademie 2010 "Codex digitalis: Optimierter Persönlichkeitsschutz – digital und vernetzt", Kiel, Germany, https://www.datenschutzzentrum.de/sommerakademie/2010/	2010-08-30	presentation	oral	National	policy makers, governmental authorities, industry, general public, journalists	301-500	ULD
Stefanie Pötzsch: "Einfluss wahrgenommener Privatsphäre und Anonymität auf Forennutzer", in U. Schroeder Ulrik (ed.): Interaktive Kulturen, LogosVerlag, Berlin, 2010	2010-09	article in proceedings	print	National	R&D		TUD
Sabrina De Capitani di Vimercati, S. Foresti, S. Jajodia, Stefano Paraboschi, Pierangela Samarati: "Fragments and Loose Associations: Respecting Privacy in Data Publishing", in Proc. of the VLDB Endowment, September, 2010	2010-09	journal article	print	International	R&D	>1000	UNIMI,UNI BG

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Claudio A. Ardagna, S. Jajodia, Pierangela Samarati, A. Stavrou: "Providing mobile users' anonymity in hybrid networks:" in Proc. 15th European Symposium on Research in Computer Security (ESORICS 2010), Athens, Greece, September, 2010	2010-09	article in proceedings	print	International	R&D	101-300	UNIMI
Sharif Tanvir Rahman: "Analyzing Causes of Privacy Mismatches in Service Oriented Architecture", Master Thesis. RWTH. September 2010	2010-09	thesis	online	National	R&D	6-10	EMIC
Yola Georgiadou, Simone Fischer-Hübner: "Surveillance and Privacy", in. What Kind of Information Society? Governance, Virtuality, Surveillance, Substainability, Resilience – Proceedings of the IFIP TC9 International Conference HCC9 2010, Brisbane/Australia, September 2010, published by Springer	2010-09	article in proceedings	print	International	R&D	301-500	kAU
Simone Fischer-Hübner: introduction to the HCC-9 stream on "Surveillance and Privacy", IFIP World Computer Congress, September, 20-23, Brisbane/Australia	2010-09	talk	oral	International	R&D	26-50	KAU
Benjamin Kellermann: "Privacy-Enhanced Single Event Scheduling", presented at SecVote 2010	2010-09-02	presentation	oral	International	R&D	26-50	TUD
Pierangela Samarati: "Protecting Privacy in Data Publishing," in Institute for Infocomm Research, Singapore, September 6, 2010	2010-09-06	talk	oral	International	R&D	11-25	UNIMI
Pierangela Samarati: "Protecting Data Privacy in Data Outsourcing and Publication", in 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore, September 7-9, 2010	2010-09-07 to 2010-09-09	keynote	oral	International	R&D	101-300	UNIMI
Harald Zwingelberg, Sven Polenz, Martin Rost and others, "Datenschutzrechtliche Leitlinien für die Erteilung von Berechtigungen nach § 21 Abs. 2 PAuswG aus Sicht der Ad-hoc-Arbeitsgruppen PA der Datenschutzbeauftragten des Bundes und der Länder" opinion of the ad-hoc working group of the German data protection authorities, 2010	2010-09-10		online	National	government authorities	500-1000	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Stefanie Pötzsch: "Einfluss wahrgenommener Privatsphäre und Anonymität auf Forennutzer", Mensch & Computer 2010, Duisburg	2010-09-12 to 2010-09-15	presentation	oral	National	R&D	301-500	TUD
Patrick Bichsel, Jan Camenisch, Gregory Neven, N.P. Smart, B. Warinschi: "Get Shorty via Group Signatures without Encryption", in Proceedings of Security and Cryptography for Networks, pp. 318-398, Springer LNCS, Vol. 6280, 2010	2010-09-13 to 2010-09-15	article in proceedings	print	International	R&D	301-500	IBM
Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati: Fragments and Loose Associations: "Respecting Privacy in Data Publishing", PVLDB 3(1): pp. 1370-1381 (2010)	2010-09-16	presentation	oral	International	R&D	26-50	UNIBG
Kai Rannenber: "Privacy ... Going, Going, Gone? The auction is in full swing" at 9th IFIP HUMAN CHOICE AND COMPUTERS	2010-09-21	presentation	oral	International	R&D	51-100	GUF
Bibi van den Berg: "Clique, or making ambiguous audiences transparent", invited talk held at CTIT Workshop on Privacy in Online Social Networks, Twente, The Netherlands.	2010-09-21	keynote	oral	Europe	R&D		TILT
Ronald Leenes: "Clique in 10 minutes"	2010-09-22	presentation	oral	International	R&D	101-300	TILT
Ronald Leenes, panel member during opening session of Smart Event 2010, Sophia Antipolis	2010-09-22	panel discussion					
Sabrina De Capitani di Vimercati: "Data Protection in Outsourcing Scenarios", in 3rd International Workshop on Autonomous and Spontaneous Security (SETOP 2010), Athens, Greece, September 23, 2010	2010-09-23	keynote	oral	International	R&D	26-50	UNIMI
M. Bezzi, S. De Capitani di Vimercati, G. Livraga, Pierangela Samarati: "Protecting Privacy of Sensitive Value Distributions in Data Release", in Proc. of the 6th Workshop on Security and Trust Management (STM 2010), Athens, Greece, September 23-24, 2010	2010-09-23 to 2010-09-24	article in proceedings	print	International	R&D	51-100	SAP,UNIMI
Pierangela Samarati: "Data Privacy in Outsourcing Scenarios," in 7th European Workshop on Public Key Services, Applications, and Infrastructures (EUROPKI 2010), Athens, Greece, September 23-24, 2010	2010-09-23 to 2010-09-24	keynote	oral	International	R&D	51-100	UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Benjamin Kellermann, Stefan Köpsell: "PrimeLife@ICT"	2010-09-27 to 2010-09-29	presentation	oral	International			many
M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Dionida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti: "A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingerprint Templates", in Proc. of the 4th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2010), Arlington, VA, USA, September 27-29, 2010.	2010-09-27 to 2010-09-29	article in proceedings	print	International	R&D	101-300	UNIMI
Marit Hansen: chair of the networking session "Identity management throughout life – solutions, trends, side effects", ICT 2010, Brussels, Belgium, http://ec.europa.eu/information_society/events/cf/ict2010/item-display.cfm?id=3435 .	2010-09-27 to 2010-09-29	conference session	oral	Europe	industry, R&D, policy makers, EC project	51-100	ULD
Rainer Böhme, Stefanie Pötzsch: "Social Lending aus der Perspektive des Datenschutzes", in F. Freiling (Ed.): SICHERHEIT 2010 – Sicherheit, Schutz und Zuverlässigkeit, LNI 170, pp. 317-328, Bonner Köllen Verlag, 2010	2010-10	article in proceedings	print	National	R&D		TUD
Stefanie Pötzsch, Peter Wolkerstorfer, Cornelia Graf: "Privacy-Awareness Information for Web Forums: Results from an Empirical Study", in Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries (NordiCHI '10), pp. 363-372, ACM, New York, 2010	2010-10	article in proceedings	print	International	R&D		TUD, CURE
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, S. Foresti, Stefano Paraboschi, Pierangela Samarati: "Supporting Privacy Preferences in Credential-Based Interactions", in Proc. of the Workshop on Privacy in the Electronic Society (WPES 2010), Chicago, Illinois, USA, October 4, 2010	2010-10	article in proceedings	print	International	R&D	51-100	UNIMI, UNI BG
Marit Hansen: "Towards future-proof privacy-respecting identity management systems", in: Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider (eds.): ISSE 2010 – Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2010 Conference, Vieweg + Teubner Verlag, Wiesbaden 2010, pp. 182-190	2010-10	article in proceedings	print	Europe	industry, R&D, policy makers	>1000	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Marit Hansen: "Geolokalisierung und Geotracking – Herausforderungen für Location Privacy", in: DANA Datenschutz Nachrichten 3/2010, pp. 100-105	2010-10	journal article	print	National	policy makers, general public	500-1000	ULD
Simone Fischer-Hübner: The Social Computer Workshop (to prepare FET Flagship proposal) , October 1, Brussels	2010-10-01	talk	oral	International	R&D	26-50	KAU
Marit Hansen: "Privacy and informational self-determination – The perspective of a German Data Protection Authority", presentation at WISSP10, Abu Dhabi, http://crissp.poly.edu/wissp10/	2010-10-04	presentation	oral	International	policy makers, R&D	11-25	ULD
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, S. Foresti, Stefano Paraboschi, Pierangela Samarati: "Supporting User Privacy Preferences on Information Release in Open Scenarios", in Proc. of the W3C Workshop on Privacy and Data Usage Control, Cambridge, Massachusetts, USA, October 4-5, 2010	2010-10-04 to 2010-10-05	article in proceedings	print	International	R&D	26-50	UNIMI,UNI BG
Jan Camenisch: "University of Luxembourg, SnT Distinguished Lecture: Minimal Data Disclosure & Identity Mixer", invited lecture	2010-10-05	talk		National	R&D		IBM
Marit Hansen: "Towards future-proof privacy-respecting identity management systems", presentation at ISSE 2010, Berlin, Germany	2010-10-05	presentation	oral	Europe	industry, R&D, policy makers	51-100	ULD
Rainer Böhme, Stefanie Pötzsch: "Social Lending aus der Perspektive des Datenschutzes", SICHERHEIT 2010 – Sicherheit, Schutz und Zuverlässigkeit, Berlin	2010-10-05 to 2010-10-07	presentation	oral	National	R&D	101-300	TUD
Marit Hansen: chair of panel discussion "Privacy Aspects of Social Networks", ISSE 2010, Berlin, Germany	2010-10-06	conference session	oral	Europe	industry, R&D, policy makers	101-300	ULD
Slim Trabelsi, Akram Njeh, Laurent Bussard, Gregory Neven: "The PPL Engine: A Symmetric Architecture for Privacy Policy Handling", W3C Workshop on Privacy and data usage control	2010-10-08	article in proceedings	online	International	R&D	>1000	SAP. EMIC, IBM
Privacy-enhanced access control in PrimeLife. Digital Identity Management Workshop, October 8, 2010, Chicago, USA.	2010-10-08	talk	oral	International	R&D	26-50	IBM

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Pierangela Samarati: "Protecting Data Privacy in Emerging Scenarios," in SBSeg 2010, Fortaleza, Brasil, October 11-15, 2010	2010-10-11 to 2010-10-15	keynote	oral	International	R&D	101-300	UNIMI
Pierangela Samarati: "Privacy in Data Publication," in SBSeg 2010, Fortaleza, Brasil, October 11-15, 2010	2010-10-11 to 2010-10-15	talk	oral	International	R&D	101-300	UNIMI
Simone Fischer-Hübner: Invited talk at Susec conference, Karlstad University, October 13	2010-10-13	keynote	oral	National	R&D	51-100	KAU
Benjamin Kellermann: "End-to-end-verifiable Voting am Beispiel von ThreeBallot und Scantegrity II", presented at Datenspuren 2010, invited talk	2010-10-16	talk		National	general public	101-300	TUD
Stefanie Pötzsch, Peter Wolkerstorfer, Cornelia Graf: "Privacy-Awareness Information for Web Forums: Results from an Empirical Study", 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries (NordCHI '10), Reykjavik	2010-10-16 to 2010-10-20	presentation	oral	International	R&D	301-500	TUD, CURE
Simone Fischer-Hübner: Invited talk at Sundsvall 42, 21 October, Sundsvall	2010-10-21	keynote	oral	National	R&D	26-50	KAU
Simone Fischer-Hübner: Invited talk at Internetdagarna, 26 October, Stockholm	2010-10-26	keynote	oral	National	R&D	101-300	KAU
Hans Hedbom: Invited talk at Internetdagarna, 26 October, Stockholm	2010-10-26	keynote	oral	National	R&D, industry	101-300	KAU
Marit Hansen: Panel participation "Fostering Innovation in Privacy Protection", OECD Conference "The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines", Jerusalem, Israel	2010-10-26	conference session	oral	International	policy makers	301-500	ULD
Marit Hansen: Chair of the panel discussion "Identity systems: Informational self determination", 32nd International Conference of Data Protection and Privacy Commissioners "Privacy: Generations", Jerusalem, Israel	2010-10-27	conference session	oral	International	policy makers	101-300	ULD
Hans Hedbom: Interview in: Computer Sweden, "Lågt intresse för integritet"	2010-10-28	interview	oral	National	R&D, industry	>1000	KAU
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, S. Foresti, T. Grandison, S. Jajodia, Pierangela Samarati: "Access Control for Smarter Healthcare Using Policy Spaces", in Computers & Security, November, 2010	2010-11	journal article	print	International	R&D	>1000	UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Simone Fischer-Hübner, Luigi Lo Iacano, Sebastian Möller: "Usable Security and Privacy", Datenschutz und Datensicherheit 11/2010	2010-11	journal article	print	National	R&D	301-500	kAU
Hans Hedbom: Presentation at IDMan 2010 in Oslo	2010-11	talk, panel discussion	oral	International	R&D	51-60	KAU
Simone Fischer-Hübner: Hans Hedbom, Tobias Pulls, Seminar at Google/Munich, 11 November 2010, Munich/Germany	2010-11-11	talk	oral	Europe	R&D	1-5	KAU
Kai Rannenber: "Privacy in personal applications", SENSIBLE/ITG/GI Workshop 2010 on Self-Integrating Systems for Better Living Environments", Wiesbaden, Germany	2010-11-12 to 2010-11-13	article in proceedings	online	International	R&D, industry, general public	51-100	GUF
Patrik Bichsel, Jan Camenisch: "Mixing Identities with Ease", in proceedings of Policies and Research in Identity Management Policies and Resesarch in Identity Management, p. 1-17, IFIP Advances in Information and Communication Technoloty, Vol. 343, 2010	2010-11-18 to 2010-11-19	article in proceedings	print	International	R&D	101-300	IBM
Patrick Bichsel: "Mixing Identities with Ease", presented at IFIP IDMAN 2010	2010-11-19	talk	oral	International	R&D	26-50	IBM
Patrick Bichsel, L. Fritsch, A. Jøsang, M. Volkamer: "Panel Discussion: Challenges in Identity Management ", at IFIP IDMAN 2010	2010-11-19	conference session	oral	International	R&D	26-50	IBM
Stefan Köpsell, Petr Svenda: "Law Enforcement and Data Retention in the light of an Anonymisation Services", Cyberspace 2011, Brno	2010-11-26 to 2010-11-28	talk	oral	International	R&D	26-50	TUD
Harald Zwingelberg: "Assessment of Privacy Issues in Monitoring Environments", talk held at meeting of the PHM Ethics project, Göttingen, Germany, November 30, 2010	2010-11-30	talk	oral	Europe	EC project	26-50	ULD
Slim Trabelsi, Akram Njeh, Laurent Bussard, Gregory Neven: "PPL Engine: A Symmetric Architecture for Privacy Policy Handling", Position paper at W3C Workshop on Privacy and data usage control, October 2010	2010-12	talk	online	International	R&D	11-25	SAP / IBM, EMIC

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Laurent Bussard, Gregory Neven, Jan Schallaböck: "Data Handling: Dependencies between Authorizations and Obligations", Position paper at W3C Workshop on Privacy and data usage control, October 2010	2010-12	talk	online	International	R&D	11-25	EMIC / IBM, ULD
Michele Bezzi: "An Information Theoretic Approach for Privacy Metrics", Transactions on Data Privacy, 3,3, 2010	2010-12	journal article	print	International	R&D	>1000	SAP
Simone Fischer-Hübner, John Sören Pettersson: "Usable privacy-enhancing Identity Management", Information and Communication Technologies, Society and Human Beings: Theory and Framework (Festschrift in honor of Gunilla Bradley), Editors: Darek Haftor, Anita Mirijamdotter, IGI Global, 2010	2010-12	book chapter	print	International	R&D	301-500	KAU
Claudio A. Ardagna, Sabrina. De Capitani di Vimercati, S. Foresti, Gregory Neven, Stefano Paraboschi, Franz-Stefan Preiss, Pierangela Samarati, Mario Verdicchio: "Fine-Grained Disclosure of Access Policies", in Proc. of the 12th International Conference on Information and Communications Security (ICICS 2010), Barcelona, Spain, December 15-17, 2010	2010-12-15 to 2010-12-17	article in proceedings	print	International	R&D	101-300	IBM, UNIBG, UNIMI
Harald Zwingelberg, representation of PrimeLife project and ABC4Trust project at SSEDIC kick-off meeting, preparing future dissemination on eID-related topics	2010-12-16	participation	oral	Europe	EC project	26-50	ULD
Harald Zwingelberg: "Identitätsmanagement, lebenslanger Datenschutz", lecture on identity management and lifelong privacy, held at the University of Applied Science Kiel, Germany	2010-12-21	presentation	oral	National	students		ULD
Slim Trabelsi: "The PPL Engine", Talk at TAS3 General Meeting	2010-15-10	talk	oral	Europe	R&D	26-50	SAP
Stuart Short, Ulrich Pinsdorf, Marc-Michael Bergfeld: "e-CV demo", ICT Event 2010 in Brussels	2010-27-09	presentation	oral	International	R&D	>1000	SAP, EMIC, G&D

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Press and Radio coverage triggered by the article of Arnold Roosendaal: "Facebook Tracks and Traces Everyone: Like This!" The news had been taken up inter alia by: Nu.nl, Volkskrant, AD, BN/DeStem, Automatisering Gids, Spitsnieuws, De Pers, NuZakelijk (plus video ANP), De Telegraaf, AdManager, Trouw, Brabants Dagblad, De Limburger, De Gelderlander, Het Parool, Holland Doc, Omroep Brabant, De Morgen (B), German Nu.nl, Asia Sun, Rima news Indonesi, Zeit Online, Stuttgarter Zeitung, LA Times, KRO Reporter (national television), Thomson Reuters	2011	interview, press- radia- and TV coverage	print	International	Europe	>1000	TILT
Stefan Schiffner, Sebastian Clauß, Sandra Steinbrecher: "Privacy, Liveliness and Fairness für Reputation", Černá et al. (eds.): SOFSEM 2011, LNCS 6543, Springer-Verlag Berlin Heidelberg, pp. 506-519, 2011	2011	article in proceedings	print	International	R&D		TUD, KU
Jaromir Dobias: "Privacy Effects of Web Bugs Amplified by Web 2.0". In S. Fischer-Hübner et al. (eds.): Privacy and Identity 2010, IFIP AICT 352, pp. 244-257, Springer, 2011	2011	article in proceedings	print	International	R&D		TUD
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, S. Foresti, S. Paraboschi, Pierangela Samarati: "Minimizing Disclosure of Client Information in Credential-Based Interactions", in International Journal of Information Privacy, Security and Integrity (IJPSI), 2011	2011	journal article	print	International	R&D		UNIMI
Sabrina De Capitani di Vimercati, S. Foresti, S. Jajodia, Stefano Paraboschi, Pierangela Samarati: "Authorization Enforcement in Distributed Query Evaluation", in Journal of Computer Security, 2011	2011	journal article	print	International	R&D	>1000	UNIMI,UNI BG
V. Ciriani, Sabrina De Capitani di Vimercati, S. Foresti, S. Jajodia, Stefano Paraboschi, Pierangela Samarati: "Selective Data Outsourcing for Enforcing Privacy", in Journal of Computer Security, 2011	2011	journal article	print	International	R&D	>1000	UNIMI,UNI BG
Sabrina De Capitani di Vimercati, S. Foresti, G. Livraga, Pierangela Samarati: "Anonymization of Statistical Data", in IT – Information Technology, January, 2011	2011	journal article	print	International	R&D	>1000	UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, E. Pedrini, Pierangela Samarati: "Privacy-Aware Access Control System: Evaluation and Decision", in Digital Privacy: PRIME – Privacy and Identity Management for Europe, Jan Camenisch, Ronald Leenes, and Dieter Sommer (eds.), Springer, 2011	2011		print	International	R&D		UNIMI
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Pierangela Samarati: "Privacy Models and Languages: Access Control and Data Handling Policies", in Digital Privacy: PRIME – Privacy and Identity Management for Europe, Jan Camenisch, Ronald Leenes, and Dieter Sommer (eds.), Springer, 2011	2011		print	International	R&D		UNIMI
Sabrina De Capitani di Vimercati, S. Foresti, Stefano Paraboschi, G. Pelosi, Pierangela Samarati: "Selective Exchange of Confidential Data in the Outsourcing Scenario", in Privacy and Identity Management for Life, Jan Camenisch, Simone Fischer-Hübner, Kai Rannenberg (eds.), Springer, 2011	2011		print	International	R&D		UNIMI,UNI BG
Michele Bezzi, Sabrina De Capitani di Vimercati, S. Foresti, G. Livraga, Stefano Paraboschi, Pierangela Samarati: "Data Privacy", in Privacy and Identity Management for Life, Jan Camenisch, Simone Fischer-Hübner, Kai Rannenberg (eds.), Springer, 2011	2011		print	International	R&D		UNIMI, SAP
Claudio A. Ardagna, Sabrina De Capitani Di Vimercati, Gregory Neven, Stefano Paraboschi, E. Pedrini, Franz-Stefan Preiss, Pierangela Samarati, Mario Verdicchio: "Advances in Access Control Policies", in Privacy and Identity Management for Life, Jan Camenisch, Simone Fischer-Hübner, Kai Rannenberg (eds.), Springer, 2011	2011		print	International	R&D		IBM, UNIBG, UNIMI
Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Pierangela Samarati: "Personal Privacy in Mobile Networks", in Mobile Technologies for Conflict Management: Online Dispute Resolution, Governance, Participation, M. Poblet (ed.), Law, Governance and Technology Series 2, Springer Science+Business Media B.V., 2011	2011		print	International	R&D		UNIMI

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Sabrina De Capitani di Vimercati, S. Foresti, G. Livraga: "Privacy in Data Publishing", in Data Privacy Management and Autonomous Spontaneous Security, J. Garcia-Alfaro, G. Navarro-Arribas, A. Cavalli, and J. Leneutre (eds.), Springer, 2011	2011	article in proceedings	print	International	R&D		UNIMI
C. Bournez, C.A. Ardagna: "Policy Requirements and State of the Art", in Privacy and Identity Management for Life, Jan Camenisch, Simone Fischer-Hübner, Kai Rannenberg (eds.), Springer, 2011	2011		print	International	R&D		UNIMI, W3C
Sabrina De Capitani di Vimercati, S. Foresti, Pierangela Samarati: "Protecting Information Privacy in the Electronic Society", in e-Business and Telecommunications International Conference (ICETE 2009), Revised Selected Papers, J. Filipe, and M.S. Obaidat (eds.), Springer-Verlag, 2010	2011		print	International	R&D		UNIMI
Pierangela Samarati: "Privacy in Emerging Scenarios of the Information Society," in MSc programme on Technoeconomic Management and Security of Digital Systems, University of Piraeus, Greece, April 23, 2011	2011	talk	oral	International	R&D	26-50	UNIMI
6th International Conference on Security and Cryptography (SECRYPT 2011), Seville, Spain, July 18-21, 2011	2011		oral	International	R&D	51-100	UNIMI
5th International Conference on Network and System Security (NSS 2011), Milan, Italy, September 6-8, 2011	2011		oral	International	R&D	51-100	UNIMI
Marc-Michael Bergfeld: Publication about "Privacy on Mobile Devices and in the Internet of the Future" on www.gi-de.com (G&D's corporate website) including references to PrimeLife	2011	journal article	online	International	general public		GD
Y. De Mulder, K. Wouters, B. Preneel: "A Privacy-preserving ID-based Group Key Agreement Scheme applied in VPAN", In SOFSEM 2011: 37th Conference on Current Trends in Theory and Practice of Informatics, Lecture Notes in Computer Science 6543, J. Hromkovič, and R. Královič (eds.), Springer-Verlag, pp. 214-222, 2011	2011	article in proceedings	print	International	R&D		KU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
F. Beato, M. Kohlweiss, K. Wouters: "Scramble! your social network data", In Privacy Enhancing Technologies International Symposium, PETS 2011, Lecture Notes in Computer Science, Simone Fischer-Hübner, and N. J. Hopper (eds.), Springer-Verlag, 15 pages, 2011	2011	article in proceedings	print	International	R&D		KU
G. Danezis, M. Kohlweiss, A. Rial: "Differentially Private Billing with Rebates", In Information Hiding, International Workshop, IH 2011, Lecture Notes in Computer Science, Springer-Verlag, 21 pages, 2011	2011	article in proceedings	print	International	R&D		KU
Peter Wolkerstorfer: "Privacy Dashboard – Gratis-Schutz vor versteckten Cookies" http://oe1.orf.at/programm/271287	2011	interview	online	National	general public	>1000	CURE
Harald Zwingelberg: "Necessary processing of personal data – The need-to-know principle and processing data from the new German identity card", to appear in: Proc. of IFIP/PrimeLife SummerSchool 2010, Springer, 2011	2011	article in proceedings	print	International	R&D, industry, policy makers, EC project	>1000	ULD
Ulrich König: "Primelife Checkout" – a Privacy enabling user interface, to appear in: Proc. of IFIP/PrimeLife SummerSchool 2010, Springer, 2011	2011	article in proceedings	print	International	R&D, industry, policy makers, EC project	>1000	ULD
Leif-Erik Holtz, Katharina Nocun, Marit Hansen: "Towards displaying privacy information with icons", to appear in: Proc. of IFIP/PrimeLife SummerSchool 2010, Springer, 2011	2011	article in proceedings	print	International	R&D, industry, policy makers, EC project	>1000	ULD
Rainer Böhme, Stefanie Pötzsch, "Collective Exposure: Peer Effects in Voluntary Disclosure of Personal Data", Financial Cryptography, St. Lucia, February 28 - March 4, 2011	2011	article in proceedings	print	International	R&D		TUD, WWU Münster
Benjamin Kellermann, Stefanie Pötzsch, Sandra Steinbrecher: "Privacy-respecting Reputation for Wiki Users", IFIP Trust Management, Copenhagen, Denmark, June 29-July 1, 2011.	2011	article in proceedings	print	International	R&D		TUD, SAP Research Dresden

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Katrin Borcea-Pfutzmann, Andreas Pfutzmann, Manuela Berg: "Privacy 3.0 := Data Minimization + User Control + Contextual Integrity", <i>it – Information Technology</i> 53/1 (2011), Oldenbourg Wissenschaftsverlag, pp. 34-40	2011-01	journal article	print	International	R&D		TUD
Stefanie Pötzsch, Katrin Borcea-Pfutzmann, Marit Hansen, Katja Liesebach, Andreas Pfutzmann, Sandra Steinbrecher: "Requirements for Identity Management from the Perspective of Multilateral Interactions", Chapter 22 in: Jan Camenisch, Ronald Leenes, Dieter Sommer (eds.): <i>Privacy and Identity Management for Europe (PRIME)</i> , Lecture Notes in Computer Science, Vol. 6545, Springer, Heidelberg, Berlin 2011, pp. 597-635	2011-01	journal article	print	International	R&D, industry, policy makers	>1000	TUD, ULD
C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "An Obfuscation-based Approach for Protecting Location Privacy", in <i>IEEE Transactions on Dependable and Secure Computing</i> , January-February, 2011	2011-01/02	journal article	print	International	R&D	>1000	UNIMI
Peter Wolkerstorfer: "Ein Kondom für den Firefox", Interview published at http://fm4.orf.at/stories/1674864/	2011-01-02	interview	online	National	general public, radio coverage	>1000	CURE
Ulrich König, Jan Schallaböck: "Privacy Preferences for E-Mail Messages" in IETF Internet-Draft draft-koenig-privicons-01	2011-01-05		online	International	standardisation body	>1000	ULD
Simone Fischer-Hübner: "Transparency enhancing tools, HCI for policy display & informed consent", contribution at the ENISA panel at CPDP 2011, Brussels	2011-01-25	panel discussion	oral	International	policy makers, industry, governmental authorities, general public, EC project	51-60	KAU

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Peter Rothenpieler, Harald Zwingelberg, Darren Carlson, Andreas Schrader, Stefan Fischer: "Sicherheit und Datenschutz im AAL Service System SmartAssist", poster presentation at 4. Deutscher AAL-Kongress 2011, Berlin, January 25-26, 2011	2011-01-25 to 2011-01-26	poster presentation	print	National	policy makers, industry, governmental authorities, general public	>1000	ULD
Marit Hansen: participation in the Conference Computers, Privacy & Data Protection CPDP 2011 with chairing of the panel discussion "What is on the law firms agenda?", Brussels, Belgium, http://www.cpdpconferences.org/	2011-01-25 to 2011-01-27	conference session	oral	International	policy makers, industry, governmental authorities, general public, EC project		ULD
Marit Hansen: contributions to the Dagstuhl Manifesto "Online Privacy" of the Dagstuhl Perspectives Workshop 11061/1, Dagstuhl, Germany	2011-02 to 2011-05	position paper	print	International	policy makers, academia, industry, governmental authorities	>1000	ULD
Marit Hansen: participation in the Dagstuhl Perspectives Workshop 11061/1 "Online Privacy", Dagstuhl, Germany.	2011-02-06 to 2011-02-11	conference session	oral	International	R&D	26-50	ULD
Harald Zwingelberg: "Schutzziele, Identitätsmanagement, lebenslanger Datenschutz", lecture on Privacy Portecion Goals, IdM and lifelong privacy, held at Wirtschaftsakademie Kiel, Germany	2011-02-17	presentation	oral	National	students		ULD
Booth presenting data protection and privacy for pupils at 1. Mini-Medien-Kompetenz Messe, February 19, 2011, Kiel, audience: pupils, parents, teachers	2011-02-19	presentation	oral	National	general public	301-500	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Consultation of a Japanese project on behalf of Japan's Government, (Ministry of Economy, Trade and Industry) on questions related to the EC data protection directive and Privacy Enhancing Technologies such as Idemix	2011-02-21	e-mail communication	print	International	government authorities, research project	unkown	IBM, ULD
Simone Fischer-Hübner, Lothar Fritsch, Erik Wästlund, Julio Angulo: "Use and Deployment of Privacy-enhancing Identity Management: Challenges to be met", under submission	2011-03	article in proceedings	print	International			KAU
Simone Fischer-Hübner: Radio Interview at SR.se, "Politikers identit�t karp�t p� n�tet"	2011-03-11	interview	oral	National	general public	>1000	KAU
Bibi van den Berg, Ulrich K�nig: "Image is everything: Audience segregation in social network sites", presentation at the Heise booth, CeBIT 2011, Hanover, Germany	2011-03-04	talk	oral	International	R&D, industry, general public	51-100	TILT, ULD
Rigo Wenning, Ulrich K�nig: "Tracking the trackers: Primelife Dashboard and dashbot", presentation at the Heise booth, CeBIT 2011, Hanover, Germany	2011-03-05	conference session	oral	International	R&D, industry, general public	51-100	W3C, ULD
Ulrich K�nig: "Privacy Icons in E-Mails", session slot on the privacy barcamp, Hanover 06.March 2011	2011-03-06	conference session	oral	National	general public	26-50	ULD
Michele Bezzi: "PrimeLife Overview & Examples of Reusable Results", Effectsplus 1st Trust and Security Clustering Meeting, Brussels, Belgium	2011-03-29	talk	oral	International	R&D, industry	51-100	SAP, IBM
Marit Hansen: Jury participation "Ideenwettbewerb Vergessen im Internet", organised by the German Federal Ministry of the Interior and acatech – National Academy of Science and Engineering (Deutsche Akademie der Technikwissenschaften), Berlin, Germany	2011-04 to 2011-10	jury participation	print+oral	National	R&D, policy makers, general public		ULD, KAU
Stuart Short, Samuel Paul Kaluvuri: "A Data-Centric Approach for Privacy-Aware Business Process Enablement", Enterprise Interoperability, Lecture Notes in Business Information Processing, Volume 76, Part 2, Part 5, 2011, pp. 191-203	2011-04-1	article in proceedings	print	International	R&D	>1000	SAP
Michele Bezzi, Slim Trabelsi: "Data Usage Control in the Future Internet Cloud", Lecture Notes in Computer Science, Volume 6656, 2011, pp. 223-231	2011-04-10	article in proceedings	print	International	R&D	>1000	SAP

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Benjamin Kellermann: "Dudle: Mehrseitig sichere Web 2.0-Terminabstimmung"	2011-04-14	talk	oral	National	R&D	11-25	TUD
Marit Hansen: "Privacy and Data Protection in Web 2.0 – The Perspective of a Data Protection Authority", Darmstadt, Germany	2011-04-28	presentation	oral	Europe	students	26-50	ULD
Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, Ge Zhang, "Privacy and Identity Management for Life", Proceedings of the 6th IFIP/PrimeLife International Summer School, Helsingborg, August 1-6, 2010, revised selected papers, published by Springer in May 2011	2011-05	Proceedings	print	International	R&D, government authorities, EC project, policy makers	301-500	KAU
Tobias Pulls, Hans Hedbom, Karel Wouters: "Logging and Privacy. It´s complicated", submitted to HotPETs	2011-05	article in proceedings	print	International			KAU
Thomas Probst, Marit Hansen: "De-Mail und Datenschutz – Gesetzliche Anforderungen, Zertifizierung und Verbesserungspotential", in: Sicher in die digitale Welt von morgen: Tagungsband zum 12. Deutschen IT-Sicherheitskongress, SecuMedia, 2011	2011-05	article in proceedings	print	National	government authorities, industry		ULD
Marit Hansen: "Datenschutz und Technik III – Datenschutzfördernde Technik", lecture at University of Kiel, Germany	2011-05-11	presentation	oral	National	students	26-50	ULD
Thomas Probst: "De-Mail und Datenschutz – Gesetzliche Anforderungen, Zertifizierung und Verbesserungspotential", presentation at BSI-Kongress 2011	2011-05-12	presentation	oral	National	government authorities, industry		ULD
Marit Hansen, Uli König, Harald Zwingelberg, Katalin Storf, Martin Rost: Workshop on Cyber-Physical Systems, Kiel, Germany	2011-05-18	presentation	oral	National	R&D	6-10	ULD
Kai Rannenber, panel expert on the FIA (Future Internet Assembly), May 18-19, 2011	2011-05-18 to 2011-05-19	panel discussion	oral	International	R&D, industry, general public		SAP
European Round Table, Brussels, Belgium	2011-05-25	presentation	oral	Europe	policy makers	51-100	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Marit Hansen: panelist at roundtable discussion "Data protection and security: How will new technologies change the policy debate?", Brussels, Belgium	2011-05-25	presentation	oral	Europe	policy makers, industry	26-50	ULD
Jan Schallaböck: "Dezentrale Soziale Netzwerke", interview for chaos radio, http://chaosradio.ccc.de/cr168.html	2011-05-27	interview	oral	International	R&D, industry, general public		ULD
Laurent Bussard, Ulrich Pinsdorf: "Abstract Privacy Policy Framework: Addressing Privacy Problems in SOA", in proceedings of iNetSec 2011, June 2011	2011-06	article in proceedings	print	International	R&D		EMIC
Harald Zwingelberg: "Necessary processing of personal data – The need-to-know principle and processing data from the new German identity card", in: Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.): Privacy and Identity Management for Life, Revised Selected Papers of 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Helsingborg, Sweden, August 2-6, 2010	2011-06	article in proceedings	print	International	R&D, government authorities, EC project, policy makers	>1000	ULD
Jan Camenisch, Simone Fischer-Hübner, Kai Rannenberg: "Privacy and Identity Management for Life", Springer, June 2011	2011-06	chapter	print	International	R&D	301-500	KAU
Ronald Leenes: "Who needs Facebook anyway? – privacy & sociality in Social Network Sites", keynote at Federated Social Web Conference, to be held June 3-5, 2011 in Berlin, Germany	2011-06-03	keynote	print	International	R&D, industry, government authorities, standardisation body	51-100	TILT
PrimeLife Project, W3C: "Federated Social Web Conference", to be held June 3-5, 2011 in Berlin, Germany	2011-06-03 to 2011-06-05	workshop	workshop	International	R&D, industry, government authorities, standardisation body	51-100	ULD, W3C

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
P. Samarati, in IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY 2011), Pisa, Italy, June 6-8, 2011	2011-06-06 to 2011-06-08	keynote	oral	International	R&D	101-300	UNIMI
Slim Trablesi, Jakub Sendor, Stefanie Reinicke, PPL: "PrimeLife Privacy Policy Engine", Policy 2011 (to be published)	2011-06-07	article in proceedings	online	International	R&D	>1000	SAP
Slim Trablesi: "PrimeLife Privacy Policy Engine", Policies for Future Internet Workshop, Pisa	2011-06-07	talk	oral	International	R&D	51-100	SAP
Jan Camenisch, Dieter Sommer: "PrimeLife Summit – Opening", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		IBM
Jan Camenisch: "Cryptography for Privacy", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		IBM
Gregory Neven: "Privacy by Policies", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		IBM
Jan Camenisch, Kai Rannenber, Rigo Wenning: "How PrimeLife creates Real-world Impact through Open Source and Standardization", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		IBM, GUF, W3C

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Simone Fischer-Hübner, Erik Wästlund, Peter Wolkerstorfer: "Usability Challenges of Privacy Technologies", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		KAU
Ulrich Pinsdorf, Marc-Michael Bergfeld, Sascha Koschinat: "Mobile and Service Infrastructures for Privacy and Identity Management", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		MS
Ronald Leenes: "The Social Web: Privacy and Information Quality", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		TILT
Katrin Borcea-Pfitzmann, Stefan Köpsell: "Exploiting the Cloud: Lifelong Privacy-preserving Data Storage", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation		International	R&D, industry, government authorities, EU commission		TUD
Pierangela Samarati: "New PETs", presentation at PrimeLife Summit Event, sub-conference of the IFIP SEC2011, Lucerne, Switzerland	2011-06-07	presentation	oral	International	R&D, industry, government authorities, EU commission		UNIMI
Benjamin Kellermann: "Privacy-Enhanced Web-Based Event Scheduling with Majority Agreement", IFIP-SEC 2011: Future Challenges in Security and Privacy for Academia and Industry	2011-06-07 to 2011-06-09	article in proceedings	print	International	R&D	301-500	TUD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Erik Wästlund, Julio Angulo, Simone Fischer-Hübner: "Evoking comprehensive Mental Models of Anonymous Credentials", accepted for iNetSec 2011, June 8, 2011, Luzern, Switzerland	2011-06-08	article in proceedings	print	International	R&D	301-500	KAU
Slim Trablesi, PPL: "PrimeLife Privacy Policy Engine", Policy 2011, Pisa	2011-06-08	talk	oral	International	R&D	51-100	SAP
PrimeLife Project, ABC4Trust Project: "Joint PrimeLife and ABC4Trust tutorial on Attribute-Based Credentials", to be held June 10, 2011 in Zurich, Switzerland	2011-06-10	workshop	oral	International	R&D, industry, government authorities, standardisation body	51-100	IBM, MS, ULD
Rigo Wenning: "La Commission européenne veut protéger notre vie privée", http://www.indexel.net/actualites/la-commission-europeenne-veut-protoger-notre-vie-privée-3383.html	2011-06-15	article	online	International	R&D		W3C
Marit Hansen: Workshop "Current and emerging challenges of eHealth – privacy, law, ethics, governance and beyond", joint workshop of PrimeLife and Middlesex University, London, UK	2011-06-16 to 2011-06-17	presentation	oral	Europe	policy makers, industry, governmental authorities		ULD
Sabrina De Capitani di Vimercati, S. Foresti, Stefano Paraboschi, G. Pelosi, and Pierangela Samarati: "Efficient and Private Access to Outsourced Data", in Proc. of the 31st International Conference on Distributed Computing Systems (ICDCS 2011), Minneapolis, Minnesota, USA, June 20-24, 2011	2011-06-20 to 2011-06-25	article in proceedings	print	International	R&D	301-500	UNIMI, UNIBG
PrimeLife workshop series: Rigo Wenning, Ulrich König "Tracking the trackers – How to see what practices websites use to collect information about us", workshop presenting the PrimeLife privacy dashboard held at Hanse-Office, Brussels, Belgium	2011-06-24	workshop	oral	Europe	journalists	11-25	ULD

Description of the Dissemination Activity	Date	Kind of activity	Type of publication	Scope	Primary type of audience	Size of audience	Partners involved
Jan Schallaböck: co-organiser of a workshop on “Privacy and Open Government data” to be held at and in co-location with the OKon 2011 in Berlin	2011-06-30 to 2011-07-01	presentation	oral	International	Community	10-20	ULD, KULeuven
Benjamin Kellermann, Stefanie Pötzsch, Sandra Steinbrecher, "Privacy-respecting Reputation for Wiki Users", IFIP Trust Management, Copenhagen, Denmark, June 29 - July 1, 2011	2011-06-29 to 2011-07-01	presentation	oral	International	R&D		TUD, SAP Research Dresden

Section B (Confidential³³ or public: confidential information to be marked clearly)

Part B1 (PUBLIC)

Exploitable knowledge

This section lists global results from the PrimeLife project. Each result is briefly described in terms of its main purpose, its content, its benefits, and its potential use. The names of all deliverables containing the described work are given.

Mechanisms

Purpose and content: This result aims at a broad adoption of privacy-enhancing and trust-enabling mechanisms and drives research in the field of cryptography, trust management, privacy of data, and access control for the protection of user-generated content.

Benefits and use: This result is research findings advancing the state of the art of current technologies and solutions. Proof-of-concept prototypes implementing novel techniques were also developed, therefore producing tools that could be used by other activities.

Availability: After project year 1 this result is available in the form of one deliverable, referenced D2.1.1 (First report on mechanisms), and four heartbeats, referenced H2.1.1 (First Report on cryptographic mechanisms), H2.2.1 (First report on user's supporting mechanisms), H2.3.1 (First report on data protection mechanisms) and H2.4.1 (First report on access control mechanisms). Furthermore, numerous research articles point to on the project website. One internal heartbeat was H6.1.1 (Report on identity management scenarios, mechanisms and protocols).

After project year 2 this result is available in form of D2.3.1 (Second report on mechanisms) as well as the heartbeats H2.1.2 (Second report on cryptographic mechanisms), H2.2.2 (Second report on user's supporting mechanisms), H2.3.2 (Second report on data protection mechanisms), and H2.4.2 (Second report on access control mechanisms). Internal heartbeats were H2.1.4 (First version of tools on cryptographic mechanisms), H2.2.4 (First version of tools on data protection mechanisms), H2.3.4 (First version of tools on data protection mechanisms), H2.4.4 (First version of tools on data protection mechanisms), and H5.2.2 (Report on research on legal policy mechanisms).

After project period 3 this result is available in form of one deliverable, D2.4.1 (Final report on mechanisms) and four heartbeats: H2.1.3 (Final report on cryptographic mechanisms), H2.2.3 (Final Report on user's supporting mechanisms), H2.3.3 (Final Report on data protection mechanisms) and H2.4.3 (Final Report on access control mechanisms). Internal heartbeats are H2.1.5 (Final report on cryptographic mechanisms), H2.2.5 (Final version of tools on user's supporting mechanisms), H2.3.5 (Final version of tools on data protection mechanisms) and H2.4.5 (Final version of tools on access control mechanisms). The details of the results can be found in scientific research publications, most of which are available on our project website.

Requirements

Purpose and content: Requirements have been elaborated for different Work Packages and tasks within PrimeLife. Especially for two demonstrators in Activity 1 and the policy language in Activity 5, legal, technical and where suitable also social requirements have been worked out. These requirements were refined by means of collaborative activities within the Work Packages. They guided the project throughout its lifetime and delivered valuable input at development stage of the prototypes.

Benefits and use: The requirements are summarised in a final public version within project year 2. The Activity 1 material is designed for project-internal discussion and for driving the prototype development and the tasks accompanying this development. The draft requirements for next generation policies have been published in order to fuel discussion at the Policy Language Interest Group (PLING) which is headed by PrimeLife partner GEIE ERCIM.

The final requirement documents discusses Privacy4Life, and Trusted Content, Social Network Services as well as Policies and will be useful for everybody interested in privacy-enhancing IdM regarding these topics.

Availability: After project year 1 this result is available in the form of four heartbeats, referenced, H1.2.5 (Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspace) and H5.1.1 (Draft requirements for next generation policies) as well as the internal heartbeats

³³ Note to be confused with the "EU CONFIDENTIAL" classification for some security research projects.

H1.1.1 (Scenario analysis, use case selection, requirements) and H1.3.2 (Draft of: Requirements and concepts for privacy-enhancing daily life). The latter is public and can be downloaded from the public website.

After project year 2 this result is available in form of H1.1.5 (Update on scenario analysis, use case selection, requirements), H1.2.5 (Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces) and H1.3.5 (Requirements and concepts for identity management throughout life). The latter heartbeat is public and can be downloaded from the public website. Further results are available in the internal heartbeat H6.3.1 (Requirements for privacy-enhancing /compliant SOAs) and the deliverable D5.1.1 (Final requirements and state-of-the-art for next generation policies).

After project year 3 this result is available in form of the heartbeats H1.3.6 (towards a Privacy-Enhanced Backup and Synchronisation Demonstrator Respecting Life-Time Aspects), H1.3.7 (Second thoughts on the WP1.3 demonstrator), H1.3.8 (Report on evaluation results of the prototype realised as D 1.3.6 as well as on the derivation of further requirements), H1.2.9 (Final report on evaluation results of the prototypes, derivation of further requirements, and extension of the prototypes) and finally H1.3.9 (Final report on analysis, scenarios, requirements, concepts and evaluation results in the areas of trusted content and privacy throughout life). Deliverable D1.3.3 (Final report on analysis, scenarios, requirements and concepts, evaluation results of "Privacy in Life") reports about the results.

Scenarios

Purpose and content: Scenarios were used in different Activities of the PrimeLife project to exemplify the problem space the project tackles in the respective Work Package and task. From the scenarios requirements were derived which in Activity 1 prepared the design of the prototype and demonstrators and in Activity 5 prepared the development of the PrimeLife policy language.

Benefits and use: The scenarios used our Activity 4 personas and put them in real-life situations, which bridged the requirements and prototype development. They contained a thorough, however not exhaustive overview of problems in IdM that PrimeLife aimed to solve within the activities.

Availability: After project year 1 scenarios were available in three heartbeats, referenced H5.1.1 (Draft requirements for next generation policies), H1.3.1 (Draft of: Analysis of privacy and identity management throughout life), H6.1.2 (Report on identity management scenarios, mechanisms and protocols) and the internal heartbeats H1.1.1 (Scenario analysis, use case selection, requirements) and H6.1.1 (Report on identity management scenarios, mechanisms and protocols).

After project year 2 scenarios were available in the internal heartbeats H1.1.5 (update on scenario analysis, use case selection, requirements) and H1.3.4 (Definition of: Prototypes of a selected realised scenario's or a meta-scenario to show the interplay between scenarios) and the heartbeat H1.3.6 (Towards a Privacy-Enhanced backup and Synchronisation Demonstrator Respecting Life-Time Aspects).

After project year 3 scenarios are available in the heartbeat H1.3.9 (Final report on analysis, scenarios, requirements, concepts and evaluation results in the areas of trusted content and privacy throughout life) and the deliverables D1.3.1 (Scenario, Analysis and Design of Privacy Throughout Life Demonstrator), D1.3.2 (Prototype of a Selected Scenario on Privacy Throughout Life), D1.3.3 (Final report on analysis, scenarios, requirements and concepts, evaluation results of "Privacy in Life"), and D6.3.3 (Scenario-based evaluation).

PrimeLife Demonstrators and Prototypes

Purpose and content: Demonstrators and prototypes were developed in order to drive the project (yearly "Focal Prototypes") and to supply privacy-enabled identity management for the whole life of people. A focus lied on trusted content, the Privacy4Life aspect and selective access control in social network services. Yearly demonstrators or prototypes illustrated privacy protection for selected scenarios. Different versions were developed through the project's lifetime and as the technology is matured during several cycles of formative evaluation. The solutions were subjected to small-scale, supervised trials with end users. The non-focal prototypes are internal results, the demonstrators and the prototypes are public results. As one specific example, the PrimeLife project partner TILT has started a social network site "Clique" as Focal Prototype for year 2 (for details on Clique see below).

Benefits and use: The prototypes show the functionality of IdM technology. They validate the project results and provide evidence that these results are suitable for exploitation from a legal, usability, and technical point of view.

Availability: After project year 1 this result was available in the form of one public deliverable, referenced D1.1.2 (First trustworthy Wiki/blog prototype), and the heartbeat, referenced H1.2.1 (Collaborative Workspace prototype). Furthermore the internal heartbeats H1.2.4 (Report on experiments with the

Collaborative Workspace prototype) and H1.1.2 (Report on experiments and evaluation results of the first Wiki/blog prototype), serve year one results.

After project year 2 this result was available in form of the heartbeats H1.1.4 (Report on experiments and evaluation results of the non-focal prototype), H1.2.6 (Development of privacy-enhancing access-control web-based service and application of that service in Social Network prototype), H1.3.7 (Second thoughts on the WP1.3 demonstrator) and H1.3.6 (Towards a Privacy-Enhanced Backup and Synchronisation Demonstrator Respecting Life-Time Aspects). Further results are available in D 1.2.2 (privacy-enabled Communities Demonstrator) and the internal heartbeats H1.3.4 (Definition of: Prototype of a selected realised scenario's or a meta-scenario to show the interplay between scenarios), H1.1.3 (non-focal prototypes), H1.2.6 (Development of privacy-enhancing access –control web-based service and application of that service in a social network prototype), H1.1.4 (Report on experiments and evaluation results of the non-focal prototype), H1.1.6 (Non-focal prototypes), H1.2.7 (Report on evaluation results of the Collaborative Workspace prototype) and H1.1.7 (Report on experiments and evaluation results of the prototypes realised).

After project year 3 this result is available in form of deliverables D1.2.2 (privacy-enabled Communities Demonstrator), D1.3.1 (Scenario, Analysis and Design of Privacy Throughout Life Demonstrator), D1.2.3 (prototype of a browser extension for a privacy dashboard) and D6.2.2 (Demonstrator on identity and trust with mobile devices) as well as heartbeats H1.2.7 (Report on evaluation results of the Collaborative Workspace prototype), H1.2.8 (privacy-enhanced access-control enabled Wiki/blog), H1.2.9 (Final Report on evaluation results of the prototypes, derivation of further requirements and extension of the prototypes), H1.3.8 (Report on evaluation results of the prototypes realised as well as on the derivation of further requirements) and H6.3.3 (Demonstrator of privacy-enhancing service composition solution). One internal heartbeat is H1.2.9 (Final report on evaluation results of the prototypes realised as well as on the derivation of further requirements).

HCI Research Reports

Purpose and content: The pattern collection summarises the HCI knowledge gathered in PrimeLife. Patterns describe context and usage of certain best-practice UI design solutions.

Benefits and use: PET developers & manufacturers can use them to design user-interfaces, which are usable. They provide descriptive solutions for implementers.

Availability: The HCI Pattern Collection is available online. After project year 1 the results are available in D4.1.1 (HCI Research Report V1) and the heartbeat H4.1.2 (HCI Pattern Collection –Version 1).

Furthermore D4.1.3 (HCI Pattern Collection Version 2) gives an update and overview after year 2.

After project year 3 this result is available in form of D4.1.5 (Final HCI Research Report

Mock-Ups and HCI Guidance

Purpose and content: The HCI Research Reports summarise the results of the HCI research conducted in PrimeLife. It contains the results of usability tests, mock-up sessions, and assurance research.

Benefits and use: The HCI research reports give insight into the mental model of end-users when it comes to PETS.

Availability: The results after project year 1 are summarised in the User Evaluation Report D4.1.1 (HCI Research Report V1) and in the internal heartbeat H4.1.2 (HCI Pattern Collection – Version 1).

D4.1.3 (HCI Pattern Collection Version 2) and D4.1.5 (Final HCI Research Report) give an update after year 2.

After project year 3, this result is available in form of D4.1.6 (Towards usable privacy-enhancing technologies: lessons learnt from the PrimeLife project).

Evaluation of PrimeLife Demonstrators and Prototypes

Purpose and content: The evaluation reports the assessment of PrimeLife demonstrators and prototypes at different levels of prototype maturity. The evaluation is performed from the legal, social, and user viewpoints. It is based on the requirements expressed for the development and provides input to the elicitation of these requirements during the next iteration.

Benefits and use: Steady evaluation is necessary in the iterative process of design and implementation to improve the concepts and prototypes of Activity 1 and to ensure the compliance with the elaborated requirements.

Availability: After project year 1 this result is available in the form of two internal heartbeats, referenced H1.1.2 (Report on experiments and evaluation results of the first Wiki/blog prototype), and H1.2.4 (Report on experiments with the Collaborative Workspace prototype).

After project year 2 this result is available within the internal heartbeat H1.1.4 (Report on experiments and evaluation results of the non-focal prototype) and later on in the internal heartbeat H1.2.7 (Report on evaluation results of the Collaborative Workspace prototype) and H1.3.7 (Second thoughts on the WP1.3 demonstrator).

After project year 3 this result is available in form of the heartbeats H4.1.3 (User Evaluation Report), H1.3.8 (Report on evaluation results of the prototype realised as D1.3.6 as well as on the derivation of further requirements) and H1.3.9 (Final report on analysis, scenarios, requirements, concepts and evaluation results in the area of trusted content and privacy throughout life). The final deliverable is D1.3.1 (Scenario, Analysis and Design of Privacy Throughout Life Demonstrator). Internal heartbeats are H1.1.7 (Final report on experiments and evaluation results of the prototypes realised), H1.2.9 (Final report on evaluation results of the prototypes, derivation of further requirements, and extension of the prototypes)

Policies

Purpose and content: This result aimed at designing security and privacy policy systems for PrimeLife. Legal and formalisation requirements have been analysed and research into new policy mechanisms is part of this result.

Benefits and use: This PrimeLife researches the relationship between data handling, access control, and trust policies. The automated negotiation, reasoning, composition, and enforcement of these three will be enabled by the PrimeLife policy language.

Availability: After project year 1 this result is available in the form of two public deliverables, D5.1.1 (Final requirements and state-of-the-art for next generation policies) and D5.2.1 (First research report on next generation policies), and one public heartbeat, referenced H5.1.1 (Draft requirements for next generation policies).

After project year 2, the result is available in the public deliverable D5.2.2 (Second research report on research on next generation policies) and heartbeat H5.2.2 (Report on research on legal policy mechanisms). Internal heartbeats were H5.3.1 (First design for policies), H5.3.2 (Second design for policies) and H5.2.1 (Report on research on policies for web service composition).

After project year 3, the result is available in D5.2.3 (Final research report on research on next generation policies).

Infrastructure

Purpose and content: PrimeLife Infrastructure results investigate the infrastructural layer without regard to specific applications (these are examined by Activity 1) but with regard to cross-cutting requirements applying to many identified scenarios. These results thus aimed at establishing the basis for the widespread deployment of privacy-enhancing mechanisms and identity management. It will identify gaps in infrastructure aspects of identity management and describe a solution that can be rolled out successfully. Touching points with existing systems were also examined.

Benefits and use: PrimeLife Infrastructure results are elaborated in order to enhance the existing infrastructure with privacy-enhancing features. IdM solutions and privacy concepts are being aligned. Infrastructure results consider economic relevance and success of the identified solution.

Availability: After project year 1 this result is available in the form of one public deliverable, referenced D6.2.1 (Infrastructure for Trusted Content), and three internal heartbeats, referenced H6.2.1 (Report on card-based Web-services), H6.1.1 (Report on identity management scenarios, mechanisms and protocols), and H6.3.1 (Requirements for privacy-enhancing/compliant SOAs).

After project year 2, this result is available in D6.1.1 (Infrastructure for Privacy-enabled Communities).

After project year 3 this result are available in D6.1.2 (Infrastructure for Identity Management Systems: Final Report) and D6.3.2 (Infrastructure for "Privacy for Life").

Dissemination Materials

Purpose and content: This result aimed at raising the visibility of the project and at ensuring dissemination and exploitation of project goals and results. Promotion material already available after project year 1 includes press releases, a flyer, a project presentation, persona posters, articles, and news messages on the project website. In the second project year, a newsletter for the Reference Group and a brochure was created. PrimeLife dissemination material introduces the problem space addressed by the PrimeLife project, and describes from various angles the project vision, approach, expected results and benefits, and status of the project consortium. Promotion material also includes mock-ups, and demonstrators.

Benefits and use: This material is designed for non-specialists. Eligible for broad distribution in the context of dissemination of the project results, it prepares and facilitates exploitation of results.

Availability: This result is available in the form of one deliverable, referenced D3.1.2 (project presentation). The parts of this result have been elaborated in the course of the project. Year 1, 2 and 3 results are made available from the project public website, and at workshops, and conferences in which the project partners participated. Several press releases have been produced. In addition, a project presentation has been prepared and presented to interested audiences such as during a NESSI meeting, the 1st PrivacyOS Conference or in a condensed version at the PrimeLife ICT Event 2008 session. Furthermore, D3.1.4 summarises the Reference Group and Peer feedback within the project.

After project year 3, further results are available in H3.1.4 (Report on cooperation activities).

Website

Purpose and content: The PrimeLife public website represents a major source for raising broad and prompt visibility of the project vision, activities, results, and the membership of the PrimeLife consortium. It provides a means to immediately inform interested audiences on progress achieved as well as events and links related to the project, to establish contacts with interested parties, and to publish project key results.

Benefits and use: The PrimeLife public website serves as a library of PrimeLife public information – including deliverables, public heartbeats, press releases, news concerning the project and relevant activities of the partners. From the second year on also papers, lectures, and presentations will be accessible by interested parties.

Availability: This result is available in the form of the deliverable D3.1.1 (Public Website). The public website is located at <http://www.primelife.eu/>. It was launched in May 2008 and will be maintained as long as deemed necessary for dissemination and exploitation of results. The website was regularly updated during and also after the project's lifetime.

Standardisation

Purpose and content: To achieve interoperability to other systems and to feed PrimeLife vision of privacy-enhancing IdM into standardisation schemes input to open standards are an important result of PrimeLife. Therefore, PrimeLife is monitoring relevant standardisation activities, and the results elaborated in PrimeLife are communicated to standardisation bodies where appropriate.

Benefits and use: PrimeLife partners who are members of standardisation bodies (GUF, KUL, ULD, W3C) can use the generated documents to put forward the standardisation supporting PrimeLife and its objectives.

Availability: After project year 1, this result is available in the form of the joint deliverable D3.3.1/D3.4.1 (First Report on Standardisation and Interoperability – Overview and Analysis of Open Source Initiatives). After project year 2, this result is available in form of the joint deliverable and heartbeat D3.4.2/H3.3.2 (Overview and Analysis of Open Sources Initiatives). For more information cf. section 0. The deliverable D3.4.3 gives a final overview on Standardisation and Interoperability. Furthermore, the First Workshop on Standardisation and Interoperability H5.4.1 was held in November 2010. A second Workshop on Standardisation and Interoperability was also held for H3.4.2, see section 0.

Open Source

Purpose and content: To ensure that the privacy community at large adopts privacy concepts and results produced by PrimeLife the project monitors and works with the relevant Open Source communities.

Benefits and use: PrimeLife considers putting project results public under a suitable open source licence to ensure broad discussion and uptake of results developed in PrimeLife.

Availability: After project year 1, this result is available in the form of the joint deliverable D3.3.1/D3.4.1 (First Report on Standardisation and Interoperability – Overview and Analysis of Open Source Initiatives). After project year 2 this result is available in form of the merged deliverable/heartbeat D3.4.2/H3.3.2 (Second Report on Standardisation and Interoperability/Overview and Analysis of Open Source Initiatives), and the heartbeats H3.3.3 (Second Contribution to Open Source) and H3.3.1 (First Contribution to Open Source). For more information, cf. section 0.

After project year 3, this result is available in form of D3.3.2 (PrimeLife Final Report on Open Source Impact) as well as heartbeat H3.3.4 (Third Contribution to Open Source).

Exploitation plans

The PrimeLife consortium consisted of 15 partners from seven member states of the European Union, Switzerland and the USA. Among them were industrial partners, one SME, research institutes, one standardisation body and one governmental data protection authority. Based on this well-balanced composition of the consortium and the partners' excellent reputation and existing network, a wide variety of dissemination activities have been carried out.

IBM Zurich Research Laboratory

For this partner there is no public version of this section available.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Together with the PrimeLife partners GUF and GEIE ERCIM the ULD is participating in standardisation activities of the project. ULD contributes to standardisation in ISO/IEC JTC 1/SC 27.

In addition ULD has made use (and will continue to do so) of PrimeLife results by communicating them into the privacy community (other DPAs and researchers) and into other national or international privacy projects. Some legal research on policies that had been jointly done as part of an ad-hoc working party of German data protection authorities could be deployed as guideline paper, which is now directly influencing the daily practice of the German authority responsible for allowing access to data stored on the newly introduced national eID card. All results are frequently used for education purposes, in particular in university lectures but also for talks directed towards high school students, parents and teachers. PrimeLife's research results have repeatedly been topic of interviews given by ULD staff, especially by Marit Hansen who is deputy director of ULD (cf. section 0). By means of the subsequent media coverage the general public is reached.

As a data protection authority one ULD's legally assigned duties is to raise awareness for privacy issues, to educate citizens and to provide consulting in privacy matters to stakeholders in the German federal state of Schleswig-Holstein. ULD will continue to deploy PrimeLife results for these tasks, e.g. by using PrimeLife knowledge but also existing dissemination material such as slide sets, flyers, PrimeLife Primers and the PrimeLife book will be used.

Technische Universität Dresden

As university at TU Dresden the main focus with respect to dissemination activities was on writing research papers, implementing concepts from these papers and making the software implemented open source for testing, evaluation and quality assurance.

The research work during the project's lifetime guided the development in the respective research fields of mechanisms supporting user's privacy and trust. For all tasks we were involved in, we contributed actively to the scientific community by writing scientific papers for conferences and workshops. The dissemination list gives an overview on these papers.

We also provided practical tools and prototypes resp. user tests demonstrating our research, especially on event scheduling, reputation systems and on privacy awareness. We make a constant effort to contribute our expertise on identity management and its application fields in scientific talks and papers as can be seen in the dissemination list. Our current work as well as future plans focus on summarising new findings in the fields of lifelong privacy, privacy awareness, and privacy-preserving event scheduling by publishing them in form of scientific articles. In addition, particular, yet unsolved issues in these areas are planned to become topics for research work of PhD students.

Karlstads Universitet

Karlstad University exploited results of the project for scientific publications and for education purposes by teaching about scientific project results within Master and PhD courses at Karlstad University and in cooperation with the Swedish IT Security Network for PhD students (SWTS), which is coordinated by Simone Fischer-Hübner. In particular project results were communicated (and will continue to do so) into the IFIP (International Federation for Information Processing) community by organising Summer School in cooperation with the IFIP Technical Committees 9 (Computer & Society) and 11 (Information Security & Privacy).

Simone Fischer-Hübner (KAU), as a member of the advisory bodies of the Swedish data protection commissioner (Datainspektionen) and the Swedish tax authorities (Skatteverket, which is in charge of developing eGovernment services) and as a member of the MSB informationssäkerhetsrad also used (and will continue to do so) PrimeLife project results to advice decision makers on privacy-enhancing technologies.

Hans Hedbom (KAU) is even after the project runtime acting as the liaison between ISO/IEC JTC 1/SC 27/WG 5 and thus monitoring and participating in the work done in WG 5. In this function, he acted as the primary information channel between PrimeLife and WG 5.

KAU has recently launched related research projects on usable identity management and transparency funded by a Google Research Award and by the Swedish KK-Foundation, which are based on KAU's research results in PrimeLife, and which will further elaborate those results for Cloud Computing and for Smart Applications. KAU also is the co-editor of the PrimeLife book, which presents the main research results from PrimeLife.

Università degli Studi di Milano

The dissemination activities by UNIMI focused on research developing novel solutions addressing the open problems related to the work packages in which UNIMI is involved. The resulting research results have been described in scientific papers that have appeared in international conferences proceedings (e.g IEEE ICDCS'09, ESORICS'09, ACM ASTACCS 2010, ESORICS 2010, PVLDB 2010, ICDCS 2011), journals (Journal of Computer Security, ACM Transactions on Database Systems, ACM Transactions on Information and System Security, IEEE Transactions on Service Computing) and as chapters in edited books. Several talks and seminars have been also delivered about the research work performed in PrimeLife. In addition, of reporting our findings in scientific publications, we have also been working on developing prototypes demonstrating the behaviour of our techniques for the realisation of access control policies with encryption.

Dissemination of project findings will continue after the end of the project through the publication of scientific papers in relevant international conferences and journals. In addition, we will continue dissemination via talks, seminars, and tutorials addressed to the research community as well as to the community at large. Prototype development has followed an open source approach allowing exploitation within open-source and standardisation activities, without ruling out a possible exploitation within commercial tools possibly developed by the industrial partners of the project.

Goethe Universität Frankfurt

The first important channel was to produce research articles and present them to the scientific community. Additionally, GUF was active in standardisation, disseminating knowledge from the project to decision makers and pushing it into international standards even beyond the project's lifetime.

The environment at Goethe University Frankfurt also allows for a direct feedback from and input to related projects, including EU-funded (PICOS, ABC4Trust), and non-EU-funded projects (e.g. funded by German Government).

Moreover, GUF plans to target students and guests of our university with teaching materials and talks even beyond the project runtime.

Tilburg University

TILT did most of its PrimeLife dissemination in journal articles, book contributions, by giving presentations, and providing posts on TILT's Law & Technology weblog. The audience will mostly consist of lawyers and social scientists.

Apart from collaboration with PrimeLife partners TILT cooperates with renowned social networks scholar Danah Boyd, researchers from the TNO Research Institute and with Prof. Tal Zarsky (Haifa University, Israel).

Ronald Leenes and Arnold Roosendal both published a chapter in the proceedings of the PrimeLife Summer School 2009 (published in 2010), while Bibi van der Berg contributed a book chapter to the PrimeLife Summer School book 2010 (in press, 2011).

Ronald Leenes wrote several book contributions and journal articles on privacy in social networks (WP1.2). In addition, a contribution was regarding compound/shared identities in the public sector (WP1.3) as well as a contribution (Journal article) on identification in eGovernment relations.

Bibi van der Berg contributed a book chapter to the PrimeLife Summer School book 2010. She and Ronald Leenes won a Best Paper Award for one of the papers presenting their work for PrimeLife at an IEEE conference in the USA in Summer 2010.

The work that was done for PrimeLife at Tilburg University also received considerable media attention. Ronald Leenes and Bibi van der Berg gave interviews with national and regional newspapers and on (live) radio.

W3C

W3C benefited from the PrimeLife project to put Privacy back on the agenda of the global technical decision making process. This included policy languages leveraging the PrimeLife results but also expanded to new

developments like "do-not-track" and the Web Identity Movement. PrimeLife results of all partners were reported on the global Workshop organised by W3C and co-branded with PrimeLife:

- Workshop on Privacy for Advanced Web APIs in London, <http://www.w3.org/2010/api-privacy-ws/>
- Workshop on Privacy and data usage control, 04/05 October 2010, Cambridge (MA, USA), <http://www.w3.org/2010/policy-ws/>
- Internet Privacy Workshop, together with the Internet, Architecture Board (IETF) 8-9 December 2010 Cambridge (MA, USA), <http://www.iab.org/about/workshops/privacy/2010-privacy-workshop-press-release.pdf>
- Workshop on Web Tracking and User Privacy, 28/29 April 2011, Princeton, NJ, USA, <http://www.w3.org/2011/track-privacy/>

Until the end of the PrimeLife project, there will be:

- - Workshop on Identity in the Browser , 24/25th May 2011, Mountain View (USA), <http://www.w3.org/2011/identity-ws/>
- Federated Social Web Summit (Identity & Privacy), Berlin 3-5 June 2011, <http://www.d-cent.org/>

During the last year of the PrimeLife project, W3C realised that the Web community wanted a much broader discussion on Privacy than was possible with the narrow charter of PLING focused on the combination of existing policy languages. W3C has closed down PLING and will open a Privacy Interest Group with a more generic profile. There is already an active publicly archived mailing-list with support from key industry players including Apple, Microsoft and Opera. This new group will pertain the starting efforts supported by PrimeLife and contribute to the Privacy considerations needed for the building of the Web Platform.

Apart from those dissemination efforts, W3C released the Dashboard and has now established an open source platform around it. <http://code.w3.org/privacy-dashboard/>

This allows the further evolution of the code after the project. During the Princeton Workshop, we have already seen a great interest in continuing development of this privacy tool.

Katholieke Universiteit Leuven

K.U.Leuven/COSIC published and presented results from WP1.2 (SNS demonstrator) and WP2.1 (trusted wallet design, cryptographic research) in international conferences, in cooperation with other PrimeLife partners. The source code, generated in WP1.2 (SNS demonstrator) was released as Open Source, after fulfilling the necessary administrative steps.

The main target of all these dissemination activities is the international research community.

Both groups of K.U.Leuven (COSIC & ICRI) have been and are involved on several projects in which privacy plays an important role: EU/PICOS, EU/TAS3, EU/Turbine, EU/PRIME. Links with several projects, and the researchers involved in them, were maintained. Moreover, K.U.Leuven has represented PrimeLife in the Cluster of European RFID Projects – CERP on the Internet of Things.

Finally, K.U.Leuven regularly hosted workshops and conferences on security- and privacy-related matters, such as:

- Workshop on Future Research Challenges for Privacy and Security in Online Social Networks, Leuven, November 5th 2009
- Interdisciplinary Privacy Course 2010, Leuven, June 23-24, 2010,
- PICOS Workshop on privacy in mobile and online social networking, Leuven, May 3rd, 201

The main objective of K.U.Leuven was to present the results, achieved in PrimeLife to the international research community, to collect feedback and connect to other researchers with similar interests. Presentations on international conferences and journal publications are the main dissemination channels to do so. National and EU-level presentations were also considered, but were a secondary objective.

The SNS prototype source code, generated in WP1.2, was being opened up other researchers to the maximum possible extent. This code may be reused as a basis for further development in follow-up projects or thesis student's work. K.U.Leuven plans to continue the line of research in the following projects: EU/SocIoS, EU/+Spaces, and IWT/SPION. K.U.Leuven/COSIC collaborated with KAU on the topic of secure and privacy-friendly logging. The results of this work are taken up for further implementation by student teams in KAU, and in a collaboration of K.U.Leuven with other Belgian research groups.

Università degli Studi di Bergamo

Dissemination activities by UNIBG within the project's lifetime focused on the writing of scientific papers for international conferences and journals. Research developed in PrimeLife on mechanisms and policies by UNIBG has been the subject of papers accepted by important conferences, like VLDB 2010, CCS 2008, IEEE ICDCS 2009 and 2011 and many others. Papers have been published in scientific journals like ACM TODS, ACM TISSEC, IEEE TSC. Chapters in scientific books were edited. Work has also been dedicated to the construction of research prototypes aiming to demonstrate the behaviour of the techniques developed within the research activity.

UNIBG in the third year of the project continued to dedicate resources to the work on research and prototype development. The production of scientific papers and research prototypes was the focus of our work, aiming at the far reaching dissemination of the results of the project, with expected significant benefits for research in information and communication technologies. These benefits should also have a positive impact on society in the large, thanks to the specific high-profile topics that the project is investigating.

The entire foreground produced by these activities became the basis for a successful exploitation within the open-source activities; the foreground produced under the responsibility of UNIBG could as well contribute to the commercial tools developed by the industrial partners of the project. UNIBG does not have at the moment plans for a direct commercial exploitation of the results. UNIBG is involved in PoSecCo, an Integrated Project of the 5th Call FP7; some of the work done by UNIBG within PrimeLife can benefit the activities within PoSecCo.

Giesecke & Devrient

Giesecke & Devrient focused on contributing to three areas of dissemination:

- General representation of the project to industry contacts, including standardisation bodies such as Global Platform (main focus) ETSI and OMTP.
- Elaboration of PrimeLife specific publications and their online publication.
- Giving industry- and university-related talks on the topic in general, the project's progress and the present and future technologies in the field.

This happened in the understanding that G&D can contribute to PrimeLife's success most by leveraging the company's industry contacts, technology base and high brand awareness in the field of security technology for the sake of the project.

Focus dissemination material: Personal presentations, articles in in-house and client / partner-related publications (online and in print), PrimeLife publications via the project's website and via G&D's global internal website.

Focus target groups: General public, standardisation bodies (esp. Global Platform, ETSI, OMTP), the firm's partners and clients, the firm's university contacts (top business schools including Harvard Business School, Judge Business School at Cambridge University, Florida international, Munich Business School and technical universities such as TU Graz, TU Munich and others).

Cooperation or exchange with other projects or researchers: Within the PrimeLife consortium. Selected conceptual findings on the PrimeLife project are to be extended in the EU-funded SEPIA project and in the future engagements regarding amongst others, cloud computing, machine to machine communication as well as mobile security payment and identity solutions..

Channels and activities for dissemination: Existing business and university contacts of the firm from 156 years of corporate history.

Firstly, G&D understands its contribution to PrimeLife as a support to the European research environment.

As a family-controlled firm, with a focus on long-term sustainable growth and entrepreneurial drive, however it is focused on continuously identifying new markets and new technologies. The findings of the PrimeLife Project will be leveraged in the conceptualisation of such in the future. For example, privacy and identity management will find increasing recognition in the firm's business of fiduciary as well as mobile technologies and services. The findings of the PrimeLife project have now been incorporated into the firm's C-TO office activities, being respected and increasingly thought about in the technology strategy of the G&D Group.

G&D strove to assure highly professional project management and fully leveraged all its contacts and knowledge base to drive the consortium's success.

Center for Usability Research & Engineering

CURE gave *HCI input* on various issues. By now HCI activities include:

- Usability laboratory evaluations with end-users
- Expert usability expert evaluation of prototypes

- Mock-ups and User Interface design for other PrimeLife activities
- HCI support and feedback for other activities

Cure also provided input to the web-site team of PrimeLife concerning the usability of the PrimeLife website. CURE used the Personas-method in PrimeLife to ensure a focus on end-users. CURE studied on the perception of Personas in PrimeLife and the modification of the personas based on the study.

For *user interface artefacts* we conducted online studies:

- Short international online studies to efficiently answer upcoming questions in a short time period
- Gather knowledge on mental models of users concerning their understanding of data transfer and data storage on Web
- Research of users understanding of privacy terms
- Final evaluation of the PrimeLife prototypes

CURE also created together with other partners of Activity 4 a pattern collection, which holds several user interface design patterns for PETs. Besides the scientific publications, the HCI pattern collection for PETs is the main dissemination result from CURE. This pattern collection was exploited by providing it to the industry.

Furthermore, CURE worked together with KAU on the development of the PET-USES questionnaire. CURE exploited the scientific knowledge for conferences and journals and contributed to the PrimeLife summer school and the PrimeLife book.

CURE's emphasis is on a user-centred approach, trying to deepen its knowledge in user requirements analysis and user evaluation, especially in the realm of privacy and privacy enhancing technologies as well as the development of interaction techniques and user interface design for privacy enhancing technologies. As a non-profit research organisation, CURE aims to develop services and related tools and concepts for its commercial spin-off USECON that focuses on usability consulting. The results from PrimeLife with respect to knowledge about the user requirements analysis and evaluation methods for PETs are utilised in order to develop strategies for the support of companies that are increasingly targeting this market.

European Microsoft Innovation Center

For this partner there is no public version of this section available.

SAP

For this partner there is no public version of this section available.

Brown University

UBR contributed to the research on cryptographic mechanisms in WP2.1. Brown University and IBM Research have a track record in cryptography for privacy and have together made substantial contributions to this field (also as part of IBM Research's work in the PRIME project). Research progress will feed back into ongoing research at Brown University and is used for dissemination particularly for education in university courses.

Part B1 (CONFIDENTIAL)

Due to PrimeLife's open strategy for disseminating our results, we did not focus on creating patents or trademarks, but rather on open communication of our results to the community.

TEMPLATE B1: LIST OF APPLICATIONS FOR PATENTS, TRADEMARKS, REGISTERED DESIGNS, ETC.					
Type of IP Rights ³⁴ :	Confidential Click on YES/NO	Foreseen embargo date dd/mm/yyyy	Application reference(s) (e.g. EP123456)	Subject or title of application	Applicant (s) (as on the application)
none					

³⁴ A drop down list allows choosing the type of IP rights: Patents, Trademarks, Registered designs, Utility models, Others.

Part B2 (CONFIDENTIAL)

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
General advancement of knowledge	Encryption policies for regulating access to outsourced data	NO	-	Personal computers, servers, outsourcing and cloud computing scenarios	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities n.e.c.	2015-2020	-	UNIBG, UNIMI
General advancement of knowledge	Fragments and loose associations for supporting privacy in data publishing	NO	-	Personal computers, servers, private data publishing, outsourcing, and cloud computing scenarios	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities n.e.c.	2015-2020	-	UNIBG, UNIMI
General advancement of knowledge	Expressive and deployable access control in open Web service applications	NO	-	Personal computers, servers, open Web-based systems, cloud computing scenarios	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities n.e.c.	2015-2020	-	UNIBG, UNIMI
General advancement of knowledge	Fragmentation of relational schemas combined with encryption for the protection of confidentiality	NO		Data outsourcing, cloud computing, storage of personal data managed by service providers	J63 - Information service activities J63.1.1 - Data processing, hosting and related activities J63.9 – Other	2015-2020	no	UNIMI, UNIBG

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
	constraints							
General advancement of knowledge	Shuffle index: private efficient access to encrypted outsourced data	NO		Data outsourcing, cloud computing, storage of personal data managed by service providers	J63 - Information service activities J63.1.1 - Data processing, hosting and related activities J63.9 – Other	2015-2020	no	UNIMI, UNIBG
General advancement of knowledge	PET-Patterns	No	-	Patterns for designing UIs of PETs	M74.1 - Specialized design activities	-	-	CURE KAU ULD
General advancement of knowledge	Heuristics for Privacy	No	-	Privacy heuristics extending the 10 usability heuristics of Nielsen	M74.1 - Specialized design activities	-	-	CURE KAU
General advancement of knowledge	Mental Model Research	No	-	Insight into users understanding of data transfer and storage on Web	M74.1 - Specialized design activities	-	-	CURE
General advancement of knowledge	Understanding of Privacy Terms	No	-	List of terms -> understanding rated on 5 item likert scale	M74.1 - Specialized design activities	-	-	CURE KAU ULD
General advancement of knowledge	Personas for Privacy	No	-	Personas deliverable	M74.1 - Specialized design activities	-	-	CURE KAU
General advancement of knowledge	PET-Uses	No	-	Questionnaire	M74.1 - Specialized design activities	--	-	CURE KAU
General advancement of knowledge	Mock-up development for different types of pet interfaces	No		Mock-Ups	M74.1 - Specialized design activities	-	-	CURE
General advancement of	PET-Patterns	No	-	Patterns for designing UIs of	M74.1 - Specialized design	-	-	CURE KAU

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
knowledge				PETs	activities			ULD
General advancement of knowledge	Heuristics for Privacy	No	-	Privacy heuristics extending the 10 usability heuristics of Nielsen	M74.1 - Specialized design activities	-	-	CURE KAU
General advancement of knowledge	Mental Model Research	No	-	Insight into users understanding of anonymous credentials	M74.1 - Specialized design activities	-	-	KAU
General advancement of knowledge	Understanding of Privacy Terms	No	-	List of terms -> understanding rated on 5 item likert scale	M74.1 - Specialized design activities	-	-	CURE KAU ULD
General advancement of knowledge	Personas for Privacy	No	-	Personas deliverable	M74.1 - Specialized design activities	-	-	CURE KAU
General advancement of knowledge	PET-Uses	No	-	Questionnaire	M74.1 - Specialized design activities	--	-	CURE KAU
General advancement of knowledge	Implementation of Data Track	No		Prototype	M74.1 - Specialized design activities J6.2.0.1 – Computer Programming Activities	-	-	KAU
General advancement of knowledge	Implementation of “Send Data?” Dialog for PPL engine	No		Prototype	M74.1 - Specialized design activities J6.2.0.1 – Computer Programming Activities	-	-	KAU
General advancement of knowledge	Implementation of PPL policy editor	No		Prototype	M74.1 - Specialized design activities	-	-	KAU

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
					J6.2.0.1 – Computer Programming Activities			
General advancement of knowledge	Implementation privacy-enhanced secure logging tools for enhancing the user's transparency	No		Prototype	M74.1 - Specialized design activities J6.2.0.1 – Computer Programming Activities	-	-	KAU
exploitation of results through (social) innovation	Prototype of a privacy preserving social network site	NO		Privacy preserving online social network site	J63.1.2 - Web portals	2011		Tilburg University (owner), software is based on GPL v2 software
General advancement of knowledge	Survey results of the need for and use of audience segregation in online SNS	NO		report/knowledge	J63.1.2 - Web portals	2011		Tilburg University, Tim Holweg (owners)
General advancement of knowledge	Knowledge on web-users' behaviour regarding online ratings	NO		report/knowledge	J63.1.2 - Web portals	2011		Tilburg University (owner)
exploitation of results through (social) innovation	Method to manage access control policies based on social groups (collections)	NO		Access control mechanism	J63.1.2 - Web portals	2011		Tilburg University (owner)

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
Open Source Software	Privacy-awareness support for forum users	No		Open source extension ("Mod") for existing open source forum-software phpBB	Social Software			TUD
General advancement of knowledge	Research results about privacy awareness of social software end users	No			M72.2.0 - Research and experimental development on social sciences and humanities			TUD
Software Prototype	Use of credentials for privacy-enhancing access control for forums			Open Source prototype for existing open source forum-software phpBB	Social Software			TUD, IBM
Commercial exploitation of R&D results	E-Voting with low requirements	no		Website, intranet solutions, hardware devices	J63.1 - Data processing, hosting and related activities; web portals			TUD
Commercial exploitation of R&D results	Anonymous Credential + Web library	no		Websites using anonymous credentials	J63.1 - Data processing, hosting and related activities; web portals			TUD, IBM
General advancement of knowledge	Demonstrator usable to demonstrate various aspects of Privacy throughout life	no	01/07/2011	Personal computers, smartphones, other computational devices	J63.1.1 - Data processing, hosting and related activities			TUD

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
Exploitation of R&D results via standards	New Standard for External an Internal APIs for TEES on Mobile Devices	NO		Mobile Devices (mobile telephones / smart phones, and also Tablet PCs, Cars, Smart Meters etc).	1. Mobile Service (esp. Loyalty, payment, banking, ticketing, medical) 2. Automotive industry 3. Machine-to-machine communication 4. Internet of the Future (secure end-to-end services)	First conceptualization of standards in 2011, full specification expected for 2012+	Potentially licensing to mobile phone vendors after further proprietary R&D is added.	Beneficiary G&D (owner) Possibility to build business models around the knowledge gained.
Commercial exploitation of R&D results	Technology for secure, trustworthy and privacy-of mobile devices	NO		See above	See above	As per 2012	Potentially licensing to mobile phone vendors after further proprietary R&D is added by G&D.	Beneficiary G&D (owner) Possibility to build business models around the knowledge gained, once additional R&D is invested by G&D.
General advancement of knowledge	Conceptual understanding of the industry dynamics and technology environment in order to create highly modularized, scalable systems that can spread, once a platform is established	NO		See above	See above, in particular, these learnings contribute to the advancement of G&D's MobiCore technology which enables secure, trustworthy application on Mobile Devices in a "Private World".	2011+	Copyrights in e.g. presentations held by G&D	Beneficiary G&D (owner)
Exploitation of results in future EU-funded	Input for SEPIA project which works	NO		See above	See above	2011-2014	Copyrights in e.g. presentations held by G&D	Beneficiary G&D (owner) and partner in SEPIA consortium

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
research	on integrating the knowledge into real mobile device platforms							
Exploitation of results in prototype	Secure and dynamic mobile services prototype in order to show solution and raise awareness	NO		See above	See above	2011+	Copyrights in e.g. presentations held by G&D	Beneficiary G&D (owner)
Commercial exploitation of R&D results	Privacy Policy Engine (part of)	YES		Platform for Service Marketplace	J63.9.9 - Other information service activities n.e.c.	2012		Owner Beneficiary SAP
General advancement of knowledge	Anonymization metrics	NO		Testing Data,	J62.0.1 - Computer programming activities	2012		Owner Beneficiary SAP
General Advancement of knowledge	1 - Research results for anonymous credentials	NO		Computational devices in general (PC, mobile, dedicated HW)	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities n.e.c.	2020	-	IBM Research, K.U.Leuven
General Advancement of knowledge	2- Scramble! Firefox plugin	NO		PC, mobile, other user devices	J63 - Information service activities	2011	(open source)	K.U.Leuven
General Advancement of	3 - Secure wallet	NO		Computational devices in general	J63 - Information service activities	2020	-	K.U.Leuven, IBM Research

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
knowledge	component: Idemix in Higgins			(PC, mobile, dedicated HW)	J63.9 - Other information service activities J63.9.9 - Other information service activities n.e.c.			
General Advancement of knowledge	4 - Smartcard assisted anonymous credentials	NO		Smart cards	J63 - Information service activities	2015		K.U.Leuven
General Advancement of knowledge	5 - Secure and privacy-friendly log trails System	NO		Computational devices in general (PC, mobile, dedicated HW)	J63 - Information service activities	2020		KAU, K.U.Leuven
Commercial exploitation of R&D results	Obligation Matching Engine	YES		Operating systems, SOA services and tools, development frameworks, workflow engines	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service activities			EMIC
Commercial exploitation of R&D results	Obligation Enforcement Engine	YES		Operating systems, SOA services and tools, development kits, workflow engines	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service activities			EMIC
Knowledge	Privacy in BizTalk	YES		Operating systems, SOA services and tools, development frameworks, workflow engines	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service			EMIC

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
					activities			
Knowledge	Usage Control	YES		Policy languages, development frameworks	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service activities			EMIC
Knowledge	Comparing policies	YES		Policy languages, development frameworks	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service activities			EMIC
Knowledge	Compliance verification	YES		Policy languages, SOA services and tools, security software, workflow engines	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service activities			EMIC
Knowledge	Formal reasoning on policies	YES		Policy languages, SOA services and tools, security software, workflow engines	J63.1 - Data processing, hosting and related activities; web portals J63.9 - Other information service activities			EMIC
Knowledge	Abstract framework for privacy policies	NO		Policy languages, SOA services and tools, security software, workflow	J63.1 - Data processing, hosting and related activities; web			EMIC

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
				engines	portals J63.9 - Other information service activities			
General advancement of knowledge	Hierarchical credential systems	NO		Personal computers, smartphones, smartcards, other computational devices	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities	2020		IBM Research, K.U.Leuven
General advancement of knowledge	Cryptographic protocols for protection of privacy in electronic interactions			Personal computers, smartphones, smartcards, other computational devices, services	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities	2020		IBM Research, K.U.Leuven
General advancement of knowledge	Cryptographic protocols for protection of privacy in electronic interactions			Personal computers, smartphones, smartcards, other computational devices, services	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities	2020		IBM Research
General advancement of knowledge	Access control method and language for privacy-preserving access control			Personal computers, smartphones, smartcards, other computational devices, services	J63 - Information service activities J63.9 - Other information service activities J63.9.9 - Other information service activities	2014		IBM Research
General	Policy engine			Personal	J63 - Information	2014		IBM Research

Type of Exploitable Foreground	Description of exploitable foreground	Confidential (YES/NO)	Foreseen embargo date dd/mm/yyyy	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
advancement of knowledge	for privacy-preserving access control			computers, smartphones, smartcards, other computational devices, services	service activities J63.9 - Other information service activities J63.9.9 - Other information service activities			

Further Details on TUD's Foreground

phpBB Privacy-Awareness Support: Personal Data MOD

MOD is short for modification, a usual concept for extension of original phpBB forum software. The objective of the Personal Data MOD is to provide information about visibility of personal data to phpBB forum users and thereby supporting users' privacy awareness.

Research results about privacy awareness of social software end users

Based the cues-filtered-out-theory, which explains human behavior in computer-mediated communication, we developed the hypothesis that additional privacy-related cues will support end users' privacy awareness and enable them to make an informed decision whether or not to disclose personal data on the Internet. This was confirmed by several user studies.

phpBB Privacy enhanced access control

This phpBB extension provides the infrastructure to implement fine-grained user-defined access control settings based on the credential system of PRIME core for either the whole forum, topics or single postings.

E-Voting with low requirements

This Web 2.0 application offers the functionality to perform small web polls, which provide (1) confidentiality (nobody may infer the results of single votes) and (2) integrity (every voter may vote only once).

Anonymous Credential + Web library

With this library, access control with anonymous credentials can be implemented in web applications easily.

Demonstrator usable to demonstrate various aspects of Privacy throughout life

The demonstrator deals with implications of lifelong privacy and identity management within the scope of the application area of protection against unwanted data loss. The proposed privacy-enhanced backup demonstrator focuses on the following problems closely linked together under the light of lifelong privacy:

- Protection of the data subject against unwanted data loss during his lifetime by redundancy and physical distribution of the data;
- Assurance of lifelong confidentiality of the data subject's data stored in a distributed environment;
- Distribution of the backup data according to different areas of life of the data subject and his different partial identities;
- Delegation of access rights to the data subject's backup data allowing other parties to operate with his data if specific conditions are fulfilled;

Further Details on K.U.Leuven's Foreground

1 - Research results for anonymous credentials

This entry refers to the research results (papers, PhD) by K.U.Leuven/COSIC regarding anonymous credentials and their use. No direct exploitation by K.U.Leuven is foreseen; most of the results are shared with IBM Research. This research topic is still evolving, and continued by K.U.Leuven.

2 - Scramble! Firefox plugin

This piece of (open source) software was developed by K.U.Leuven/COSIC. It allows to encrypt information on – in theory – any html-based social network site, for a specified set of recipients, using PGP as an encryption means. COSIC plans to develop this demonstrator in follow-up research. Exploitation is limited to providing expertise wrt the software, as it is open source. Potential impact: if a social network site decides to embrace this or similar technology, it can improve the privacy of all their customers.

3 - Secure wallet component: Idemix in Higgins

In this demonstrator, K.U.Leuven/COSIC tries to facilitate the use of Idemix anonymous credentials in the Higgins framework. Similarly to the Scramble plugin, exploitation remains limited due to the open source character. The impact will be accelerated adoption of anonymous credentials in the Higgins community.

4 - Smartcard assisted anonymous credentials

K.U.Leuven/COSIC developed a demonstrator in which anonymous credentials are backed up by a smart card. This knowledge and expertise will be used and progressed in COSIC's further research wrt eID cards and hardware solutions. Impact remains limited, as it concerns bleeding-edge technology.

5 - Secure and privacy-friendly log trails system

Together with KAU, K.U.Leuven/COSIC has been developing a secure privacy-friendly logging system to log actions on PII. The system allows Data Subjects to build a log trail of actions on their PII. This research topic is still evolving, and continued by K.U.Leuven and KAU. Potential impact is improved transparency for Data Subjects, in several application domains, including healthcare and egovernment.

Further Details on GD's Foreground

The above shown overview is a summary of the lessons learned that G&D has derived from the PrimeLife project. The insights of the project and the prototype development will empower the firm to create technology and embed this technology into Mobile Device platforms that are widely spread throughout the devices in the market. G&D's MobiCore technology will profit from the insights developed in PrimeLife. The technology will enable future Mobile Devices to offer applications that are secure, trustworthy and can be enhanced with privacy features. The results of PrimeLife (including the demonstrator) will be used to present the concept of isolated "private worlds" to the market players in order to raise awareness and support the diffusion of the MobiCore technology. If MobiCore succeeds, also by referring to the PrimeLife research, then a Europe will have created a new de facto standard in the Mobile Device industry and how privacy and identity is used in this context.

Further Details on EMIC's Foreground

Obligation Matching Engine allows comparing the obligation parts in data-handling policy. It could be used with or without PPL to negotiate obligations in privacy or broader usage control scenarios. Exploitation would require additional R&D effort.

Obligation Enforcement Engine could be extended in order to enforce obligations (data retention, notifications, etc.) for different personal data storages (database, file system, cloud). Exploitation would require additional R&D effort.

Privacy in BizTalk: we've collected considerable experience how to build privacy-aware privacy-enhancing, cross-domain SOA applications with Microsoft BizTalk Server 2009 and Windows Communication Foundation. We have several example applications and best practices. Some of the findings have been distilled into the Privacy Lifecycle (cf. PrimeLife deliverable D6.3.2). Exploitation would require additional R&D effort.

Usage Control: the concept of nested usage control could be used in different context (privacy, right management, etc.). Exploitation would require additional R&D effort.

Comparing Policies: We've worked on comparing individual pieces of policies. The concept of similarity of policies could be reused for other policy languages. Exploitation would require additional R&D effort.

Compliance verification: In WP5.2 we've worked on comparing execution traces (e.g. log files) and policies. This could be reused in other contexts as well, i.e. without PPL. Exploitation would require additional R&D effort.

Formal reasoning on policies: In WP5.2 we developed a prototype that allowed reasoning on policies. In order to do that we had to translate multiple domain-specific languages into a unified model. Some aspects of the translation can be applied to other policy languages and other types of models. Exploitation would require additional R&D effort.

Abstract framework for privacy policies: In WP6.3 we've distilled best practices for privacy-compliant cross-domain SOA into an abstract framework. This framework will influence further development of privacy policies and their usage in SOA.

4.3 Report on societal implications

A General Information <i>(completed automatically when Grant Agreement number is entered.</i>	
Grant Agreement Number:	216483
Title of Project:	Privacy and Identity Management in Europe for Life
Name and Title of Coordinator:	Dieter Sommer
B Ethics	
1. Did your project undergo an Ethics Review (and/or Screening)? <ul style="list-style-type: none"> If Yes: have you described the progress of compliance with the relevant Ethics Review/Screening Requirements in the frame of the periodic/final project reports? <p>Special Reminder: the progress of compliance with the Ethics Review/Screening Requirements should be described in the Period/Final Project Reports under the Section 3.2.2 'Work Progress and Achievements'</p>	No
2. Please indicate whether your project involved any of the following issues (tick box) :	YES
RESEARCH ON HUMANS	
• Did the project involve children?	no
• Did the project involve patients?	no
• Did the project involve persons not able to give consent?	no
• Did the project involve adult healthy volunteers?	yes
• Did the project involve Human genetic material?	no
• Did the project involve Human biological samples?	no
• Did the project involve Human data collection?	yes
RESEARCH ON HUMAN EMBRYO/FOETUS	
• Did the project involve Human Embryos?	no
• Did the project involve Human Foetal Tissue / Cells?	no
• Did the project involve Human Embryonic Stem Cells (hESCs)?	no
• Did the project on human Embryonic Stem Cells involve cells in culture?	no
• Did the project on human Embryonic Stem Cells involve the derivation of cells from Embryos?	no
PRIVACY	
• Did the project involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	yes
• Did the project involve tracking the location or observation of people?	no
RESEARCH ON ANIMALS	
• Did the project involve research on animals?	no
• Were those animals transgenic small laboratory animals?	no
• Were those animals transgenic farm animals?	no
• Were those animals cloned farm animals?	no
• Were those animals non-human primates?	no
RESEARCH INVOLVING DEVELOPING COUNTRIES	
• Did the project involve the use of local resources (genetic, animal, plant etc)?	no
• Was the project of benefit to local community (capacity building, access to healthcare, education etc)?	no
DUAL USE	
• Research having direct military use	no

• Research having the potential for terrorist abuse		no
C Workforce Statistics		
3. Workforce statistics for the project: Please indicate in the table below the number of people who worked on the project (on a headcount basis).		
Type of Position	Number of Women	Number of Men
Scientific Coordinator	0	1
Work package leaders	4	2
Experienced researchers (i.e. PhD holders)	17	28
PhD Students	13	17
Other	0	1
4. How many additional researchers (in companies and universities) were recruited specifically for this project?		
Of which, indicate the number of men: 10 total, of which 6 men		

D Gender Aspects

5. Did you carry out specific Gender Equality Actions under the project? Yes
 No

6. Which of the following actions did you carry out and how effective were they?

	Not at all effective	Very effective
<input type="checkbox"/> Design and implement an equal opportunity policy	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>
<input type="checkbox"/> Set targets to achieve a gender balance in the workforce	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>
<input type="checkbox"/> Organise conferences and workshops on gender	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
<input type="checkbox"/> Actions to improve work-life balance	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>
<input type="radio"/> Other: <input style="width: 200px;" type="text"/>		

7. Was there a gender dimension associated with the research content – i.e. wherever people were the focus of the research as, for example, consumers, users, patients or in trials, was the issue of gender considered and addressed?

Yes- please specify

No

E Synergies with Science Education

8. Did your project involve working with students and/or school pupils (e.g. open days, participation in science festivals and events, prizes/competitions or joint projects)?

Yes- please specify summer schools, courses in schools and at university

No

9. Did the project generate any science education material (e.g. kits, websites, explanatory booklets, DVDs)?

Yes- please specify: Yes- please specify: a book and tutorials

No

F Interdisciplinarity

10. Which disciplines (see list below) are involved in your project?

Main discipline³⁵: 1.1

Associated discipline³⁵: 5.2

Associated discipline³⁵: 5.4

G Engaging with Civil society and policy makers

11a Did your project engage with societal actors beyond the research community? (if 'No', go to Question 14) Yes
 No

11b If yes, did you engage with citizens (citizens' panels / juries) or organised civil society (NGOs, patients' groups etc.)?

No

Yes- in determining what research should be performed

Yes - in implementing the research

Yes, in communicating /disseminating / using the results of the project

³⁵ Insert number from list below (Frascati Manual).

11c In doing so, did your project involve actors whose role is mainly to organise the dialogue with citizens and organised civil society (e.g. professional mediator; communication company, science museums)?	<input type="radio"/> <input type="radio"/>	Yes No
12. Did you engage with government / public bodies or policy makers (including international organisations)		
<input type="radio"/> No <input checked="" type="checkbox"/> Yes- in framing the research agenda <input checked="" type="checkbox"/> Yes - in implementing the research agenda <input checked="" type="checkbox"/> Yes, in communicating /disseminating / using the results of the project		
13a Will the project generate outputs (expertise or scientific advice) which could be used by policy makers? <input checked="" type="checkbox"/> Yes – as a primary objective (please indicate areas below- multiple answers possible) <input checked="" type="checkbox"/> Yes – as a secondary objective (please indicate areas below - multiple answer possible) <input type="radio"/> No		
13b If Yes, in which fields?		
Agriculture Audiovisual and Media Budget Competition Consumers (x) Culture Customs Development Economic and Monetary Affairs Education, Training, Youth Employment and Social Affairs	Energy Enlargement Enterprise Environment External Relations External Trade Fisheries and Maritime Affairs Food Safety Foreign and Security Policy Fraud Humanitarian aid	Human rights Information Society (x) Institutional affairs Internal Market Justice, freedom and security (x) Public Health Regional Policy Research and Innovation (x) Space Taxation Transport

13c If Yes, at which level?		
<input checked="" type="checkbox"/>	Local / regional levels	
<input checked="" type="checkbox"/>	National level	
<input checked="" type="checkbox"/>	European level	
<input checked="" type="checkbox"/>	International level	
H Use and dissemination		
14. How many Articles were published/accepted for publication in peer-reviewed journals?		190 (peer-reviewed articles in journals and papers in proceedings)
To how many of these is open access³⁶ provided?		estimated > 85%
How many of these are published in open access journals?		
How many of these are published in open repositories?		mostly open repositories, such as authors' webpages
To how many of these is open access not provided?		
Please check all applicable reasons for not providing open access:		
<input checked="" type="checkbox"/> publisher's licensing agreement would not permit publishing in a repository <input type="checkbox"/> no suitable repository available <input type="checkbox"/> no suitable open access journal available <input type="checkbox"/> no funds available to publish in an open access journal <input type="checkbox"/> lack of time and resources <input type="checkbox"/> lack of information on open access <input type="checkbox"/> other ³⁷ :		
15. How many new patent applications ('priority filings') have been made? <i>("Technologically unique": multiple applications for the same invention in different jurisdictions should be counted as just one application of grant).</i>		0
16. Indicate how many of the following Intellectual Property Rights were applied for (give number in each box).	Trademark	0
	Registered design	0
	Other	0
17. How many spin-off companies were created / are planned as a direct result of the project?		0
<i>Indicate the approximate number of additional jobs in these companies:</i>		0
18. Please indicate whether your project has a potential impact on employment, in comparison with the situation before your project:		
<input type="checkbox"/> Increase in employment, or	<input type="checkbox"/>	In small & medium-sized enterprises
<input type="checkbox"/> Safeguard employment, or	<input type="checkbox"/>	In large companies

³⁶ Open Access is defined as free of charge access for anyone via Internet.

³⁷ For instance: classification for security project.

<input type="checkbox"/> Decrease in employment, x Difficult to estimate / not possible to quantify	<input type="checkbox"/> None of the above / not relevant to the project
19. For your project partnership please estimate the employment effect resulting directly from your participation in Full Time Equivalent (FTE = one person working fulltime for a year) jobs:	<i>Indicate figure:</i> 33 FTE in PrimeLife consortium
Difficult to estimate / not possible to quantify	<input type="checkbox"/>
I Media and Communication to the general public	
20. As part of the project, were any of the beneficiaries professionals in communication or media relations?	
x Yes	<input type="radio"/> No
21. As part of the project, have any beneficiaries received professional media / communication training / advice to improve communication with the general public?	
x Yes	<input type="radio"/> No
22 Which of the following have been used to communicate information about your project to the general public, or have resulted from your project?	
x Press Release	x Coverage in specialist press
x Media briefing	x Coverage in general (non-specialist) press
<input type="checkbox"/> TV coverage / report	x Coverage in national press
x Radio coverage / report	x Coverage in international press
x Brochures /posters / flyers	x Website for the general public / internet
<input type="checkbox"/> DVD /Film /Multimedia	<input type="checkbox"/> Event targeting general public (festival, conference, exhibition, science café)
23 In which languages are the information products for the general public produced?	
x Language of the coordinator	x English
x Other language(s)	

Question F-10: Classification of Scientific Disciplines according to the Frascati Manual 2002 (Proposed Standard Practice for Surveys on Research and Experimental Development, OECD 2002):

FIELDS OF SCIENCE AND TECHNOLOGY

1. NATURAL SCIENCES

- 1.1 Mathematics and computer sciences [mathematics and other allied fields: computer sciences and other allied subjects (software development only; hardware development should be classified in the engineering fields)]
- 1.2 Physical sciences (astronomy and space sciences, physics and other allied subjects)
- 1.3 Chemical sciences (chemistry, other allied subjects)
- 1.4 Earth and related environmental sciences (geology, geophysics, mineralogy, physical geography and other geosciences, meteorology and other atmospheric sciences including climatic research, oceanography, vulcanology, palaeoecology, other allied sciences)
- 1.5 Biological sciences (biology, botany, bacteriology, microbiology, zoology, entomology, genetics, biochemistry, biophysics, other allied sciences, excluding clinical and veterinary sciences)

2 ENGINEERING AND TECHNOLOGY

- 2.1 Civil engineering (architecture engineering, building science and engineering, construction engineering, municipal and structural engineering and other allied subjects)
- 2.2 Electrical engineering, electronics [electrical engineering, electronics, communication engineering and systems, computer engineering (hardware only) and other allied subjects]
- 2.3. Other engineering sciences (such as chemical, aeronautical and space, mechanical, metallurgical and materials engineering, and their specialised subdivisions; forest products; applied sciences such as geodesy, industrial chemistry, etc.; the science and technology of food production; specialised technologies of interdisciplinary fields, e.g. systems analysis, metallurgy, mining, textile technology and other applied subjects)

3. MEDICAL SCIENCES

- 3.1 Basic medicine (anatomy, cytology, physiology, genetics, pharmacy, pharmacology, toxicology, immunology and immunohaematology, clinical chemistry, clinical microbiology, pathology)
- 3.2 Clinical medicine (anaesthesiology, paediatrics, obstetrics and gynaecology, internal medicine, surgery, dentistry, neurology, psychiatry, radiology, therapeutics, otorhinolaryngology, ophthalmology)
- 3.3 Health sciences (public health services, social medicine, hygiene, nursing, epidemiology)

4. AGRICULTURAL SCIENCES

- 4.1 Agriculture, forestry, fisheries and allied sciences (agronomy, animal husbandry, fisheries, forestry, horticulture, other allied subjects)
- 4.2 Veterinary medicine

5. SOCIAL SCIENCES

- 5.1 Psychology
- 5.2 Economics
- 5.3 Educational sciences (education and training and other allied subjects)
- 5.4 Other social sciences [anthropology (social and cultural) and ethnology, demography, geography (human, economic and social), town and country planning, management, law, linguistics, political sciences, sociology, organisation and methods, miscellaneous social sciences and interdisciplinary, methodological and historical S1T activities relating to subjects in this group. Physical anthropology, physical geography and psychophysiology should normally be classified with the natural sciences].

6. HUMANITIES

- 6.1 History (history, prehistory and history, together with auxiliary historical disciplines such as archaeology, numismatics, palaeography, genealogy, etc.)
- 6.2 Languages and literature (ancient and modern)
- 6.3 Other humanities [philosophy (including the history of science and technology) arts, history of art, art criticism, painting, sculpture, musicology, dramatic art excluding artistic "research" of any kind, religion, theology, other fields and subjects pertaining to the humanities, methodological, historical and other S1T activities relating to the subjects in this group]