PrimeLife
Dissemination Report V1

Editors:	Marit Hansen (ULD)
	Maren Raguse (ULD)
	Harald Zwingelberg (ULD)
Reviewers:	Mario Verdicchio, (UNIBG)
	Christian Weber, (GUF)
Identifier:	H3.1.1
Type:	Heartbeat
Class:	Public
Date:	27 February 2009

Abstract

PrimeLife's first project year has resulted in several public reports and many dissemination activities of the consortium. This report presents the project's dissemination and exploitation activities during the first project year. It describes the target groups relevant for PrimeLife, and it documents the exploitation and dissemination strategies and actions designed to reach these target groups in the context of competition.

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe – Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

List of Contributors

Contributions from several PrimeLife partners are contained in this document. The following list presents the contributors for the chapters of this deliverable.

Chapter	Author(s)
Introduction	Harald Zwingelberg (ULD), Maren Raguse (ULD)
1.1 PrimeLife project objectives	Harald Zwingelberg (ULD)
1.2 PrimeLife use and dissemination	Harald Zwingelberg (ULD), Maren Raguse (ULD)
2.1 Results to be disseminated	Maren Raguse (ULD), Rigo Wenning (W3C), Hans Hedbom (KAU)
2.2 Exploitable knowledge	Maren Raguse (ULD), Peter Wolkersdorfer (CURE)
2.3 partner-specific exploitation plans	all partner representatives
3 Exploitable results	Dieter Sommer (IBM)
4 Publishable Results	Harald Zwingelberg (ULD)
Introduction	Harald Zwingelberg (ULD), Maren Raguse (ULD)

List of acronyms

APDCM	La Agencia de Protección de Datos de la Comunidad de Madrid
BEUC	The European Consumer's Organisation
CA	Consortium Agreement, California
CEN	European Committee for Standardization
CERP	Cluster of European RFID Projects
CNIL	Commission Nationale de l'Informatique et des Libertés
D	Deliverable
Daidalos II	Designing Advanced network Interfaces for the Delivery and Administration of Location Independent, optimised personal Services
DPA	Data Protection Authority
EC	European Commission
EnCoRe	Ensuring Consent and Revocation
ENISA	European Network and Information Security Agency
EPTA	European Parliamentary Technology Assessment Association
ETSI	European Telecommunications Standards Institute
EU	European Union
EuroPriSe	European Privacy Seal
FIDIS	Future of Identity in the Information Society
FP7	Framework Programme 7
GA	Grant Agreement
H	Heartbeat
HCI	Human-Computer Interaction
ICT	Information and Communication Technology
IdM	Identity Management
IEC	International Electrotechnical Commission
IFIP	International Federation for Information Processing
IGF	UN-Internet Governance Forum
IP	Intellectual Property
IPCA	Intellectual Property consortium agreement
IPR	Intellectual Property Right
ISO	International Organisation for Standardisation
IST	Information Society Technologies
IT	Information Technology

ITU	International Telecommunication Union
JTC1	Joint technical committee 1
MOBIO	Mobile Biometry
NESSI	Networked European Software & Services Initiative
NGO	Non-governmental organisation
OASIS	Organisation for the Advancement of Structured Information Standards
OMTP	Open Mobile Terminal Platform
PhD	philosophiæ doctor (doctor of philosophy)
PET	Privacy-Enhancing Technology
PICOS	Privacy and Identity Management for Community Services
PLCA	PrimeLife Consortium Agreement
PLING	Policy Language Interest Group
PR	Public Relation
PRIME	Privacy and Identity Management for Europe
PrivacyOS	Privacy Open Space
R&D	Research & Development
RESERVOIR	Resources and Services Virtualization without Barriers
SC	Subcommittee
SME	Small and medium-sized enterprises
SNS	Social Network Services
SOA	Service Oriented Architecture
SVN	Subversion
SWIFT	Secure Widespread Identities for Federated Telecommunications
TAM	Tivoli Access Manager
TAS3	Trusted Architecture for Securely Shared Services
TFIM	Tivoli Federated Identity Manager
TU	Technische Universität
UK	United Kingdom
USA	United States of America
V	Version
W3C	World Wide Web Consortium
WA	Washington
WG	Working Group
WP	Work Package

Contents

List of Figures

List of Tables

Chapter *1*

Introduction

In the PrimeLife Dissemination ReportV1 the partners report on their activities to publicise their research findings and knowledge generated within the project (foreground) during the recent project period. The partners further state their plans to exploit the generated knowledge and by which means they might have taken up on the exploitation activities already.

This Dissemination Report V1 provides a picture of the activities undertaken during the first project year. It will be updated accordingly after the second project year (V2, H3.1.2) and at the end of the project (V3, H3.1.3).

This document consists of three sections:

- Results to be disseminated
- Exploitable results
- Publishable results

This chapter introduces PrimeLife's project objectives, target audiences and the dissemination strategy to reach these audiences. A central role in the dissemination activities is the project's web site where publishable results will be available for download: http://www.primelife.eu/

1.1 PrimeLife project objectives

The overall objective in PrimeLife is to help enable individuals to retain control over their personal information. The PrimeLife predecessor project PRIME already identified several emerging challenges in the field of identity management and provides first solutions by means of user centric identity management systems. While these were sufficient in traditional server-client style transactions PrimeLife addresses challenges to privacy and identity management induced by the fundamental changes to the internet as they currently occur. These changes comprise inter alia the change to a more community based focus with interactions mainly happening between comprising 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. But contributing to these collaborative internet services may cause a live long trail of personal data.

PrimeLife tackles these challenges by working 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 has set up an effective and efficient management that drives the project towards meeting these objectives. The partners formed six activities consisting of multi-disciplinary research teams which will focus on the following specific objectives all aiming at making sustainable privacy, trust and identity management a reality:

To reach the goal of providing and supporting privacy throughout our lives PrimeLife will perform 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.

Privacy can not be provided for our scenarios with today's privacy technologies. PrimeLife will therefore perform the basic and applied technological research that is required to make privacy throughout life a reality. Important technology areas that PrimeLife covers are:

- **Tools**: The emerging Internet needs to be built on scalable and usable privacy technology components. Examples include privacy-enhancing cryptography, trust establishment mechanisms, and 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. We will show how to make privacy technologies usable by all groups of citizens.
- **Policies**: In order to provide configurable privacy spheres, it is important to build privacy policy support into all 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. We will show how to provide scalability and privacy.

Finally, the project aims 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, the project contributes to:

- **Open Source** initiatives,
- engaging in **standardisation bodies**, and
- providing **educational material**.

Reaching the objectives requires extensive dissemination activities. PrimeLife pursues this goal by its dissemination strategy as described within the following section.

1.2 PrimeLife use and dissemination strategy

In accordance with PrimeLife's long-term goal to protect privacy of individuals over their whole lifespan, dissemination of the project's findings takes a central role. Reflecting its importance the consortium devotes Activity 3 "Privacy Live – Transferring results into practice" to this goal. PrimeLife puts strong effort on dissemination activities based on a PR strategy which needs to be agreed upon among the consortium partners. Activity 3 will coordinate the dissemination of results, set up the public web site and organise central outreach activities (like press releases, representation of PrimeLife at important events, organisation of public workshops). In addition, and as a general principle, each partner is responsible and encouraged to publish individual results.

Activity 3 "Privacy Live" has a central role in the project dissemination activities and is well incorporated in the network of other activities. Activity 1 aims at a life-long protection of privacy in the emerging collaborative internet. The activity will research and define the requirements as an input for the research activities. Activities 2, 4, 5 and 6 build the actual privacy technologies. This includes basic research as well as applied research constructing privacy tools, privacy policies and privacy-enabled infrastructures. Activity 3 aims at the exploitation of the results. It provides the research findings for the real world. Its goals are to transfer PrimeLife's research results into open source, standards and actual products that will enable privacy protection in future technologies. The project expects that by doing so, we will discover some gaps and requirements which Activity 3 will feed back to the relevant work packages.

An overview of the information flow and the incorporation of the work packages on dissemination of which Activity 3 consists is given in the figure below:

Figure 1: Activity 3 and dependencies
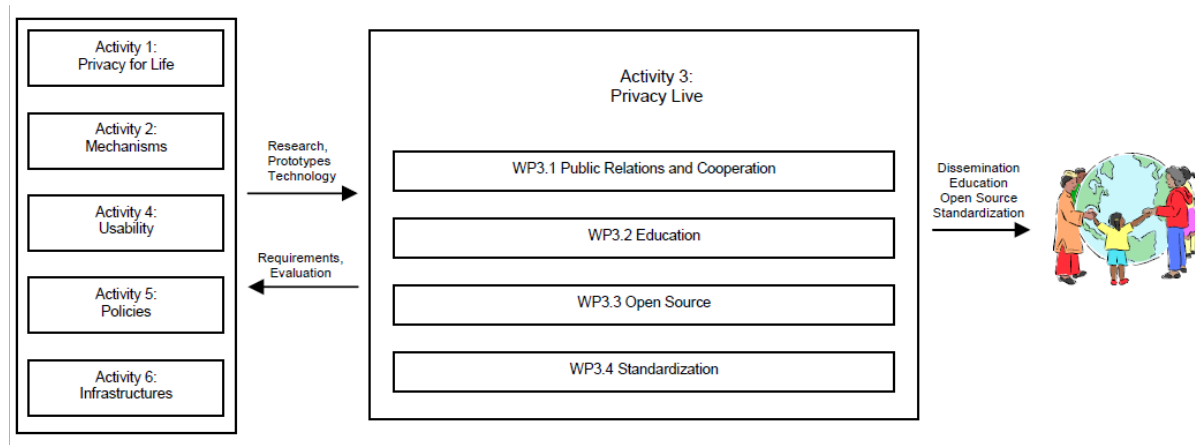
PrimeLife raises the privacy awareness of the general public by means of summer schools, a book publication and lectures. As the book on the PrimeLife research results (D3.2.1) intends to summarize the project's findings it is consequently scheduled for the end of the project (month 36). Contributions to the book will not be available before the end of the third project year.

PrimeLife partners engage actively in educating students and the general public. Current developments, arising challenges and the solutions user centric identity management and the underlying technologies may provide had been topic at a variety of lectures held by PrimeLife partners.

1.3 Exploitation directions

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

- *Open Source Software*: The consortium encourages the use of research results including the developed prototypes as the basis for products which are released via an Open Source licence. This is reflected in an own a separate Work Package (WP3.3). For more details see section 2.5 below.
- *Commercialised products or services*: The industry partners may pick up project results to build on top own products or services.
- *Think tank*: The PrimeLife partners make 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 exploit the project's results via elaborating scientific publications.
- *Educational material*: PrimeLife supports the preparation of high-quality educational material (courses, text books, etc.) and their use in teaching and raising awareness. At present several academic partners and ULD use PrimeLife foreground for lectures at universities.
- *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 keeps close contact with several EC-funded and national projects. Research findings are exchanged on conferences, by personal contact between researchers. Due regard is held to the recent deliverables and publications of other projects.
- *Standardisation*: The project aims to influence standardisation initiatives. To this end, it reaches out to relevant communities as part of Work Package 3.4, and offers appropriate results for standardisation. (see 2.4 below)

The following key results will be object of further exploitation. Please refer to section 2.8 below for further detail on the awaited results.

- Mechanisms
- Requirements
- Scenarios
- PrimeLife Demonstators 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 varies, e.g. the industry partners pursue other goals than the academic partners, NGOs or privacy protection authorities.

1.4 Motivations and goals

When the predecessor project PRIME started in March 2004, the PRIME partner's motivation for extensive dissemination activities was that many people had not been aware that their privacy is at stake in many situations and even if they were, they had not been able to protect themselves. This has changed. Due to several scandals concerning the loss and fraudulent exploitation of private data in different European countries (in particular in Germany and Great Britain) and critical reports of the European Data Retention Directive in the specialised press the citizens are much more aware of their needs to protect their privacy. Several newspapers report about ways and possibilities to protect ones privacy and the need of identity management.

However, deeper knowledge as well as effective and transparent, easy to use tools for identity management currently are missing and the perception of privacy issues varies considerably between member states and age groups.

1.5   Target audience

The success of PrimeLife and beyond in the area of privacy and identity management will primarily rely 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 permanent community of stakeholders are crucial. The following stakeholders have been identified:

- *Individuals,* who are end users and/or data subjects (so-called usees, 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. Users should be educated about the use of personal data and the deployment of PrimeLife applications. Therefore the usability of PrimeLife tools is an important precondition for allowing users to utilise them.
- *Media / Journalists*, especially those specialised in information and communication technology should help 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).
- *User and consumer associations* at national and European level like the European Consumer's Association (BEUC). Also the co-operation with user/consumer FP7-ICT-2007-1 PrimeLife Version 2, 26/09/2007 GA no. 216483 16 associations will be helpful to elicit user's requirements for PrimeLife-based solutions. In addition they could be helpful in advertising privacy seals and other methods of privacy assurance, increasing both awareness and visibility concerning PETs in products. Education staff, curricular policy makers, and educational associations and institutions to use e.g., PrimeLife educational material in schools, universities and other teaching environments.
- *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 should be informed at regular intervals about PrimeLife and because of that they should use their influence to 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, technology assessment organisations at national and European level, like European Parliamentary Technology Assessment Association (EPTA). They should be stimulated to co-operate 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 usees), 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 will be important for the transfer of PrimeLife results into standardisation to ensure interoperability with existing systems and concepts.

- *System developers, system designers, suppliers of ICT products and services* should be motivated to see PETs as a business enabler and to integrate PrimeLife FP7-ICT-2007-1 PrimeLife Version 2, 26/09/2007 GA no. 216483 17 concepts and solutions into their systems and products. Thereby they can 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 is also needed for a broad deployment of PrimeLife-based solutions within organisations. They have to be well 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 usees. 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 the stakeholders participates in the PrimeLife Reference Group.

1.6 Reaching the target audiences

PrimeLife is using standard dissemination channels for scientific results, such as articles in journals, papers at conferences and demonstrations at fairs, as well as making use of new ways to disseminate results, e.g., directly to users in communities or by providing Open Source software. In recognition of the overall importance of the dissemination strategy the consortium chose the approach considered the most effective by combine 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 are 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 consist of:

- PrimeLife's website
- networking activities
- Summer Schools
- Standardisation workshops
- Workshops for journalists
- Cooperation workshops
- PrimeLife's internal website

The PrimeLife workshop series enables 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 are choosing the dissemination channels that fit best to the target groups which have been addressed by the partners in a long history of research networking. Taking a geographical dimension into account the general public is usually addressed by national dissemination. The following table gives an overview of suitable communication channels for reaching different target audiences.

	Communication channels	Target audiences						
		Potential users and customers	Organisations and third parties	Media	Standardisation committees	Research community	PrimeLife Partners	European Commission
Permanent	Media	√	√	√	√	√	√	√
	Public events	√	√	√		√	√	√
	Partners' own channels	√	√	√	√	√	√	
	Technical publications			√	√	√	√	√
Specific	Public web site	√	√	√	√	√	√	√
	Networking activities					√		
	PrimeLife-specific events	√	√	√		√	√	√
	Internal web site						√	

Table 1: Communication channels to reach target audiences

1.7 Workshop series

PrimeLife plans to organise five different kinds of workshops:

- Workshops for the PrimeLife Reference Group to get feedback on results achieved by PrimeLife results so far ("Reference Group Meetings");

- Summer Schools for researchers and students to teach about state-of-the-art and new results and trends on privacy-enhancing identity management;
- Standardisation Workshop addressing 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 can discuss their own needs for PET modules and pick up PrimeLife's results to improve their own concepts and IT systems.
- The workshops function as interaction means with relevant stakeholders grouped by their main interest. Per workshop the appropriate PrimeLife partners to present project results and to elicit the desired feedback will be recruited.
- 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 which PrimeLife foresees also for the future, the project is organising "Cooperation Workshops" where mainly specific questions of interested projects should be discussed. By this means, PET concepts developed within PRIME or PrimeLife can be tailored according to the needs of the other projects and be used in their specifications and applications.

1.7.1.1   PrimeLife Reference Group Meetings

The PrimeLife project established an external expert panel, the Reference Group, which consists of representatives of relevant stakeholders: consumer organisations, data protection authorities, industry, academia, NGOs, and EC authorities. The Reference Group consists of 29 members.

The First Reference Group Meeting will take place from 23 to 24 March 2009 in Frankfurt, Germany. PrimeLife partners, mainly Work Package and Activity leaders will use the opportunity to gain expert feedback on results and ongoing research in PrimeLife. The Reference Group members will get insight into work ongoing in PrimeLife. However, the goal of the workshops with the Reference Group is 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 will be sought by the consortium.

Feedback of the Reference Group will be presented in the report D 3.1.4 Summary of Reference Group Feedback, due in month 20.

1.7.1.2   PrimeLife/IFIP Summer School 2009

During its duration PrimeLife will organise two summer schools. Task 3.2.1 is lead by Karlstad University who has comprehensive experience in organising summer schools for PRIME and FIDIS jointly with IFIP (International Federation for Information Processing).

From 7th-11th September 2009, PrimeLife WP 3.2 will hold an International 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.

In 2007 and 2008, the FIDIS (Future of Identity in the Information Society) FP6 Network of Excellence had already successfully organised international Summer Schools in cooperation with IFIP. This series of international Summer Schools organised jointly with IFIP will now be continued by PrimeLife. 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 theme of the PrimeLife/IFIP Summer School 2009 will be on privacy and identity management for emerging Internet applications throughout a person's life.

The aim of the Summer School 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 will be invited and will be given in the morning sessions. In the afternoons, there will be 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 are solicited by a Call for Contributions that was circulated in December 2008. Contributions will be selected based on an extended abstract review by a Summer School Programme Committee.

The Summer School Website is available at: http://www.it.kau.se/IFIP-summerschool/

Accepted short versions of papers will be made available to all participants in the Summer School Pre-Proceedings. After the Summer School, authors will have 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 will again be reviewed and selected by the Summer School Programme Committee.

1.7.1.3 Standardisation Workshop

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

W3C organized a W3C Workshop on the Future of Social Networking[1] 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![2] from TILT and Semantic enhancements for social networks[3] from W3C. The Workshop Report[4] 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.org[5]. PrimeLife will further contribute to this effort as social networks are one of the core use cases of PrimeLife.

This first workshop on standardisation issues focused on the following core-activities:

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

Further activities are planed for the upcoming project years. The close interaction with the Policy Language Interest Group will be continued.

---

[1] http://www.w3.org/2008/09/msnws/
[2] http://www.w3.org/2008/09/msnws/papers/tilt.pdf
[3] http://www.w3.org/2008/09/msnws/papers/policy-ih-rw.html
[4] http://www.w3.org/2008/09/msnws/report
[5] http://lists.w3.org/Archives/Public/public-social-web-talk/

The PrimeLife project envisions holding a standardisation workshop during the final project year. For details on the ongoing dissemination efforts by PrimeLife to standardisation bodies see 2.4 below.

1.7.1.4 Workshops for journalists

PrimeLife plans to hold a workshop for journalists to explain the project's result and position the project in the identity management landscape. As it is depending on the project's results this workshop will be held at the end of the project.

1.7.1.5 Cooperation Workshops with related projects

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 seeks to assist other European projects in assuring privacy-enhancing identity management and other privacy enhancing techniques are considered and focused on. PrimeLife is in contact with more than 10 EU research projects and initiatives.

PrimeLife attended the first Open Space conference of the EU funded project PrivacyOS in Strasbourg from 13 to 15 October 2008. PrivacyOS is a European project aimed at bringing together industry, SMEs, Government, 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 EU 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.

PrimeLife organized a cluster event of FP7 projects together with the Commission as a joint workshop on 25 February 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. PrimeLife partners IBM, EMIC, ULD and GUF participated in this workshop.

PrimeLife organised a session at the ICT event 2008 in Lyon on 27 November 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.

Chapter 2

Results to be disseminated

2.1 Dissemination of Foreground

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

In this chapter we give an overview on PrimeLife dissemination activities, thus refining the project's dissemination strategy being introduced in section 1.2. The second section describes dissemination to the public, while the third section concentrates on the research community. The fourth section shows PrimeLife's outreach to standardisation bodies and initiatives. The fifth section deals with PrimeLife and open source. The sixth section describes how PrimeLife addresses EC channels to disseminate results.

2.2 Dissemination to the public

One of the project objectives is to raise awareness for privacy and identity management issues and possible solutions. Therefore disseminating PrimeLife's results to the public is considered very important by all consortium members. The following table shows the main results of the dissemination efforts to the public made in project year 1.

Planned / actual dates	Type	Type of audience	Countries addressed	Partner responsible / involved
	Web site			
In the beginning of the project (May 2008)	Project web site	General public	All	ULD / GEIE ERCIM / all

21

Planned / actual dates	Type	Type of audience	Countries addressed	Partner responsible / involved
	Press releases:			
In the beginning of the project (27 May, 2008)	Press release "European Union launches 16 Million Euro R&D Project on Privacy and Identity Management"	General public	All	ULD / all
	Flyers / Leaflets / Posters / Presentation Slides / Exhibition:			
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 organized 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 annually	CeBIT exhibition in Hanover, Germany	General public, IT specialists	All	ULD / all

Table 2: Overview of dissemination actions addressing the public

2.3 Dissemination to research

PrimeLife is a research project and therefore 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 first year's research report of Activity 2, referenced D2.2.1 (First report on mechanisms), the first year'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).

PrimeLife is designing and implementing demonstrators and prototypes to understand and address privacy issues in emerging real-life scenarios. Legal and technical requirements are elaborated to facilitate privacy-enhancing identity management solutions.

This prototyping is supported by research Work Packages which 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 has eight of these research Work Packages. The first one, WP2.1 is concerned with cryptographic mechanisms, the fifth, WP2.2 works on mechanisms supporting privacy and trust, the sixth, WP2.3 deals with privacy of data, the seventh, WP2.4 researches access control for the protection of user-generated content, the eighths, WP4.1 is about UI representation of privacy-enhancing IdM concepts, the ninths, WP4.2 works on trust and assurance HCI, the tenths, WP4.3 is concerned with user interfaces for policy display and administration, the finally the elevenths, WP5.2 focuses on research on next generation policies.

For the first project year, 22 scientific publications were produced by the research Work Packages, cf. D2.2.1 (First Report on Mechanisms).

2.4 Standardisation

Standardisation efforts in PrimeLife mainly target the International Standardisation Organisation (ISO), the UN-Internet Governance Forum (IGF) and the World Wide Web Consortium (W3C).

ISO/IEC JTC 1/SC 27/WG 5 is currently working on a number of standards relating to PrimeLife activities.

The main effort in W3C Standardization is directed towards the Policy Languages and Interest Group (PLING)[6]. PLING itself serves as a coordination platform for further liaisons to other groups and other Standardization organizations.

W3C also has an active Working Group on Geolocation[7] that has a large debate over privacy protection. PrimeLife will try to influence this group to get a higher level of data protection and the relevant hooks to apply PrimeLife solutions to Geolocation scenarios.

2.5 PrimeLife and Open Source

The aim of PrimeLife is to make Privacy Real, which requires supporting and triggering a broad uptake of privacy-enhancing solutions for IdM developed by PrimeLife. In order to achieve broad acceptance and roll-out of PrimeLife results the project aims at ensuring that the community at large adopts privacy technologies. To this effect PrimeLife will work with the relevant Open Source communities. Already in month three an analysis of relevant Open Source and standardisation initiatives was made. Based on this

---

[6] http://www.w3.org/Policy/pling/
[7] http://www.w3.org/2008/geolocation/

analysis the project is currently deciding to which of these initiatives it will collaborate with and to what extent.

2.6 PrimeLife addressing EC channels

PrimeLife plans to and has made 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.

EC-funded projects have approaching PrimeLife to get consulting on specific questions regarding privacy and identity management.

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".

2.7 PrimeLife dissemination activities

PrimeLife organised a session at the ICT event 2008 in Lyon on 27 November 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.

2.8 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. Also results which are not available after project year 1 are described.

2.9 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 will be research findings advancing the state of the art of current technologies and solutions. Proof-of-concepts prototypes implementing novel techniques will also be developed, therefore producing tools that can 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), H 2.2.1 (First report on user's supporting mechanisms), H 2.3.1 (First report on data protection mechanisms), and H 2.4.1 (First report on access control mechanisms), and numerous research articles which are pointed to on the project web site.

2.10 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 will be refined by means of collaborative activities within the Work Packages. They aim at guiding the project throughout its lifetime and at delivering valuable input at development stage of the prototypes.

Benefits and use: The requirements at this stage of the project are mostly internal documents which will see a final public version within project year 2. Currently 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 will discuss 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 three heartbeats, referenced H1.1.1 (Scenario analysis, use case selection, requirements), H1.3.2 (Draft of: Requirements and concepts for privacy-enhancing daily life), and H5.1.1 (Draft requirements for next generation policies). The latter is public and can be downloaded from the public web site.

2.11 Scenarios

Purpose and content: Scenarios are 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 are derived which in Activity 1 prepare the design of the prototype and demonstrators and in Activity 5 prepare the development of the PrimeLife policy language.

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

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

2.12 PrimeLife Demonstrators and Prototypes

Purpose and content: Demonstrators and prototypes are developed in order to drive the project and to supply privacy-enabled identity management for the whole life of people. A focus lies on trusted content, the Privacy4Life aspect and selective access control in social network services. Yearly demonstrators or prototypes illustrate privacy protection for selected scenarios. Different versions will be developed through the project's lifetime and as the technology is matured during several cycles if formative evaluation. The solutions will be subjected to small-scale, supervised trials with end users. The non-focal prototypes will be internal results, the demonstrators and the prototypes will be public results.

Benefits and use: The prototypes show the functionality of IdM technology. They aim to 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 is available in the form of one public deliverable, referenced D1.1.2 (First trustworthy Wiki/blog prototype), and one internal heartbeat, referenced H1.2.1 (Collaborative Workspace prototype).

2.13 HCI Research Reports

Purpose and content: The pattern collection summarizes the HCI knowledge gathered in PrimeLife. Patters describe context and usage of certain best-practise 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 will be available online.

2.14 Mock-Ups and HCI Guidance

Purpose and content: The HCI Research Reports summarize 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 will are summarised in the User Evaluation Reports D4.1.1 and D4.1.5.

2.15 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).

2.16 Policies

Purpose and content: This result aims 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. The development and implementation of a versatile PrimeLife policy language is envisioned.

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 one public deliverable, referenced D5.2.1 (First research report on next generation policies), and one public heartbeat, referenced H5.1.1 (Draft requirements for next generation policies).

2.17 Infrastructure

Purpose and content: PrimeLife Infrastructure results investigate the infrastructural layer without regard to specific applications (these are examined by Activity1) but with regard to cross-cutting requirements

applying to many identified scenarios. These results thus aim 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 will also be 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).

2.18 Dissemination Materials

Purpose and content: This result aims 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 will be 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 and will be elaborated in the course of the project. Year 1 results are made available from the project public web site, and at workshops, and conferences in which the project partners participated. So far one press release has 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.

2.19 Web site

Purpose and content: The PrimeLife public web site 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 web site 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 web site 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.

2.20 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, GEIE ERCIM) 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). For more information cf. section 2.4.

2.21 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 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). For more information cf. section 2.5.

2.22 Further dissemination plans

The PrimeLife consortium consists of 15 partners from 7 member states of the European Union, Switzerland and the USA. Among them are 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 in project year 1 and are planned for the upcoming two years. The partners will also use their individual channels where appropriate to exploit and disseminate foreground. Industry partners plan in particular to use the findings in their product development while academic partners will disseminate the knowledge in scientific publications.

Chapter 3

Publishable Results

This section provides a publishable overview of exploitable results PrimeLife has generated within the first project year. Downloads of the published deliverables are available on PrimeLife's website: http://www.primelife.eu/deliverables

Identifier	Name	Date	status
D1.1.1	Analysis of existing identity-related web protocols	August 2008	published
D1.1.2	First trustworthy wiki/blog prototype	November 2008	published
H1.3.2	Draft of: Requirements and concepts for privacy-enhancing daily life	February 2008	finalized
D2.1.1	First report on mechanisms	February 2008	finalized
H2.2.1	First report on user's supporting mechanisms	February 2008	finalized
H2.3.1	First report on data protection mechanisms	February 2008	finalized
H2.4.1	First report on access control mechanisms	February 2008	finalized
D3.1.1	Public website	March 2008	published
H3.1.1	PrimeLife dissemination report V1	February 2008	finalized
D3.1.2	Project presentation	June 2008	published
D3.3.1	Overview and Analysis of Open Source Initiatives	May 2008	published
H3.3.1	First Contribution to Open Source	February 2008	finalized
D3.4.1	First Report on Standardisation and Interoperability	May 2008	published
D4.1.1	HCI Research Report - Version 1	February 2008	finalized
H4.1.2	HCI Pattern Collection – Version 1	February 2008	finalized
H5.1.1	Draft requirements for next generation policies	December 2008	published
D5.2.1	First research report on next generation policies	February 2008	finalized
D6.2.1	Infrastructure for Trusted Content	August 2008	published
D7.1.3	Y1 publishable summary	February 2008	To be published

Table 3: Publishable Results, Year 1