Final Report on Standardisation and Interoperability

Editors: Rigo Wenning, (W3C)
Hans Hedbom, (Karlstads Universitet)

Identifier: D3.4.3
Type: Deliverable
Class: Public
Date: May 23, 2011

Abstract

As expected, the standardisation efforts in PrimeLife did not end up in large specification work, but rather in stimulating the Internet community into thinking more about privacy risks and challenges. PrimeLife contributed successfully to get Privacy back as a top item on the world's ICT agendas. It did so by organizing very successful workshops. The success forced PrimeLife to organize more workshops than initially planned in the description of work.

PrimeLife also contributed to the more abstract standardisation efforts going on in ISO. There the basic Privacy framework is elaborated and formalized into specifications. The liaison established with ISO/IEC SC27 WG 5 allowed PrimeLife to add major results into the framework developed in this venue.

Finally, Partner G & D provided an API specification to the Global Platform, an SDO for secured environment applications.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483 for the project PrimeLife.

SEVENTH FRAMEWORK PROGRAMME

Members of the PrimeLife Consortium

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

List of Contributors

This deliverable has been jointly authored by multiple PrimeLife partner organisations. The following list presents the contributors for the individual parts of this deliverable.

Chapter	**Author(s)**
Executive Summary	Rigo Wenning
Internet Standardisation	Rigo Wenning
ISO Standardisation	Hans Hedbom, Jan Schallaböck
TEE Specification	Marc-Michael Bergfeld

Executive Summary

PrimeLife has significantly participated in standardisation. It reached out to two communities working rather independent of each other: The ISO standardisation in ISO/IEC SC27 WG 5 on the one hand and the W3C/IETF community specifying Internet technologies.

At ISO, PrimeLife established formal liaisons and benefited from those liaisons to get deep insight into the work of SC27. Kai Rannenberg from PrimeLife Partner GUF acts as the convener of WG 5 while Jan Schallaböck from ULD is providing the Secretariat with significant contributions from Hans Hedbom working for Partner Karlstads Universitet. Finally, G&D also invested significantly into the ISO standardisation.

The actions around Internet standardisation were mainly of exploratory nature. PrimeLife was supposed to organize 2 workshops, but at the end of the project it will have organized seven! This was partly due to the success of the first workshops organized, but also because of the political landscape in the EU and the US that had put the Privacy topic high on the agenda. PrimeLife was instrumental in implementing this political agenda. All fell together when the industry and the research community asked for further opportunities to meet and discuss Privacy because of the way W3C and PrimeLife organized the thought provoking explorations by bringing a truly international audience together in one venue.

Contents

Chapter 1

Introduction

The primary aim of standardization in a social and economic context is to help encouraging the free movement of goods. Standardization will help to remove technical barriers, open up new markets, and enable new economic models. It helps to create economies of scale while at the same time increasing opportunities for product differentiation and competition and services. Consequently, standardization may help establish compatibility and interoperability, it may enable market self-regulation, and guard the safety and health of citizens.

Standardisation has many goals and facets: Standards are used for consumer protection to achieve a minimum quality of certain products and services. Standards lead to lower cost because of a unified higher volume market. But in ICT, standardisation is mainly about Interoperability. Why?

Eric von Neumann was the last man to know every detail from the CPU to the application programming and he died in 1957. Since then, the ICT landscape is characterized by an extensive labour divide between specialists. The device driver programmers rely on the information that the device manufacturers give them. The operating system developers rely on information and interfaces that are provided by the device drivers and by the CPU instruction set. Application developers rely on the interfaces from the operating system and Web developers rely on the interfaces the Web provides. This means that ICT has a much larger need for agreed information that leads to interoperability. In short, ICT needs many more standards than the rest of the industry.

Chapter 2

The functionality of standardisation in ICT

The function of standards in ICT goes far beyond pure interoperability. A new set of interfaces are sometimes the way to open an entire new world thus creating new markets. Apart from its social achievements, the Web created a huge new market that contributed enormously to economic prosperity, but it did not take into account the constraints of the mobile world. It took new standards to bring the Web to mobile devices thus creating a huge new market for applications and commerce. Now we see mobile applications and web applications catered to mobile phones, location dependent services and web pages that display well on desktop computers and on mobile phones alike.

Quite often, an idea capable to create such new markets comes out of research. But often researchers lack the tools, the contacts or the motivation to actually create the market. Resources are calculated to show that it theoretically should work and perhaps provide a demonstrator to showcase how it could look like. At the same time, people from industry don't take the time to understand the potential of an idea. The European Commission realized this gap and consequently has recently put a lot of emphasis on the relation between research and standardisation[1]. The PrimeLife standardisation work has to be seen in this tradition. Here, standardisation is providing the necessary platform to organize a joint development for areas that are too large for one single stakeholder.

And there is traditional industry standardisation that also applies to ICT. Here, standardisation is rather focused on achieving agreement in mature markets. This means several vendors had some competition and the products have converged sufficiently to formalize the common understanding of how things should be done. This will create a level playing field and take the competition to the next higher level.

1 For further information on research and standardisation see http://copras.org/

Finally, standardisation is used by public authorities to achieve goals of consumer protection. In this context, minima are defined by a standards developing organization (SDO) and laid out in a technical specification that is then cited by regulation. This has several advantages over simple direct regulation. Normally, the SDO tasked with the standardisation is the one that has technical expertise in the area. Second best is that the SDO tries to bring the relevant stakeholders and technical experts around the table. The process of an SDO allows to guide and funnel the -sometimes controversial- discussions towards a consensus. So here, standardisation serves to organize a social dialog across geographic boundaries to ease the finding of a common understanding for the Internet that crosses those geographic boundaries.

PrimeLife developed activities and generated impact on all those flavours. The ISO standardisation focused on high level framework and platform specifications that contain requirements on privacy friendly software design. The exact meaning of “Privacy by design” as promoted by Ann Cavoukian, the famous Ontario (Canada) Privacy Commissioner remains to be defined. The ISO work as furthered by PrimeLife has helped to gain a lot of understanding in this area. It is very much geared towards the consumer protection goals and rather caters to regulation. But it is also very useful for industry in order to help develop products and services in line with sane privacy principles.

The W3C work was concentrated around enduring the dialogue between Web developers, browser makers and researchers, understanding privacy issues of the Web, presenting possible solutions and searching for a possible consensus with the Web community. Furthermore, the Web discussion was extended into the IETF to address Privacy issues on the deeper layers in the stack, traditionally addressed by them and thus positioning Privacy as an issue for Internet architecture. This means, W3C addressed the concrete low level mechanics of privacy tools, privacy messaging, data collection, tracking and opt out. It brought the Privacy topic back high on the agenda of the relevant technical experts and stakeholders who, today, decide and work towards the Web and the Internet of tomorrow.

Chapter 3

Internet Standardisation

PrimeLife has researched on Social Networking. It has looked into long term aspects of Privacy in life from birth to bury that touch on eGovernment. For the policy research and the infrastructure questions, it has dealt with the service world. All those objects of our research are relying heavily, if not exclusively, on Web technologies and its underlying stack of Internet technologies.

There are several ways to start or contribute to Internet standardisation. W3C usually organizes workshops to test the momentum in a certain community to agree on a common set of technologies. Those workshops are rather oriented towards standardisation of existing technologies in a mature technical environment where the parties have already settled. But W3C also organizes exploratory workshops. Those workshops have as a goal to bring the world's leading experts around a table to find out more about a given issue. Both types of workshops can result in a set of further tasks that the community recommends as next steps to W3C.

Despite the rather old legal framework in the EU, Privacy on the fast evolving Internet and on the Web is not well understood. This means the research challenge does not only consist in finding how to achieve a known and desired goal, but it also means that not all the challenges are known and on the table. Most of the standardisation workshops were of exploratory nature. This positions them close to the scientific workshops done and also to the very successful summerschools organized by PrimeLife. But they still have their merit as the standardisation community can have a different view on the same topic because there, also industry constraints and the installed base are factored into the expressed opinions and positions. This allows for a much better insight on what may be possible within a certain realm of scientific solutions.

3.1 W3C Workshop on Access Control Application Scenarios, Luxembourg 2009[2]

Privacy enhancing technologies are great consumers of access control technology. PrimeLife is in no way an exception here. The early works and research on the PrimeLife model and policy engine consequently focused on access control and how to organize it. At the same time, with some help of the European Commission, a coordination with other projects was organized. Rapidly after the first PrimCluster meetings it became clear that all projects were using and extending the Extended Access Control Language (XACML) specified by OASIS. Further inquiry in the community revealed that there were more projects beyond the ones organized in PrimCluster which had new ideas and innovative extensions concerning XACML. The topic was brought up in the Policy Languages Interest Group (PLING) to determine interest from the industry. The response was positive. PrimeLife decided to allocate the necessary resources for a workshop on Access Control Application Scenarios that would look specifically in XACML innovations and beyond. W3C organized the workshop as a standardization workshop[3].

The workshop brought worldwide research and user communities together to explore evolving application scenarios for access control technologies, such as XACML. Results form a number of recent European research projects in the grid, cloud computing, and privacy areas were presented. Especially PrimeLife Partner Università degli Studi di Milano showed how to extend these technologies beyond classical intra-enterprise applications.

The Workshop on Access Control Application Scenarios attracted 20 position papers of rather diverse nature. Most of them were presented in the two day workshop in Luxembourg and the discussion converged towards 4 topics:

- Attributes
- Sticky Policies
- Obligations
- Credential based Access Control

3.1.1 Attributes

XACML provides a framework for access control systems in heterogenous IT landscapes. There is a protocol and some basic requirements that are common to all access control systems. But XACML does not specify the semantics of the conditions that have to be fulfilled to grant access. Those semantics are specified by the actual implementer within an existing enterprise. This means in order to expand to inter-enterprise interoperability or to wider use on an Internet scale, XACML needs semantics filling out its own framework that makes access control conditions predictable and interoperable even where there was no prior agreement on the semantics of the access control

2 http://www.w3.org/2009/policy-ws/

3 All the proceedings, minutes and papers are available under http://www.w3.org/2009/policy-ws/

conditions. University Bergamo and Milano contributed a paper describing extensions to XACML to make it easily deployable and suitable for open Web-based systems.

The participants presented their vocabularies during the Workshop. PrimeLife presented a privacy vocabulary. UPC presented access control in social networking using FOAF and MPEG 21 REL together to get the necessary semantics while using XACML for the policies. Other work on attribute vocabularies for export control, geospatial data and health care data were presented in the workshop. The chair invited all participants to contribute their semantics to the TC XACML that could act as a clearing house for those ontologies. This way, duplication of attributes could be avoided and a cleared vocabulary could be standardized for a wider audience and to achieve some basic interoperability for web or inter-enterprise consumption.

3.1.2 Credential based Access Control

Credential based Access Control would allow for a more privacy friendly access control system that would also be more widely useable on the Web. The aim is to prove only selected attributes as need for the task at hand. There is already a large set of literature on capabilities, but XACML currently does not have the ability to identify the type of credential used nor to specify, which credential is needed to get access to a certain resource. This is more or less a special case of the attributes topic with additional protocol issues. One way to convey the credential would be to use SAML, but SAML only allows XML Signature as a proof token.

Further steps in this direction are already undertaken and the actual PrimeLife protocol will be contributed to TC XACML to address credentials as access control conditions. But the contribution will also make XACML itself more privacy friendly. Today, if a user hits an access controlled resource, the system just returns that this resources is restricted. The user then tries as many credentials as he has until the resource opens. The XACML 2.0 protocol has no way to tell the user which credential it requires to open the access to the desired resource. The PrimeLife extension enables the PDP to convey the type of credential it wants already in the response to the initial attempt to access a resource.

3.1.3 Sticky Policies

Applying access control scenarios beyond the borders of a well-walled enterprise does not only raise the question about agreed and interoperable access control semantics. It also raises the question on how to make sure that all users of a data record can respect the access restrictions if this record is traveling around from service to service, across company borders or from continent to continent on the web. One solution is known under the name “Sticky Policy”. This means that there is a persistent link between the access control information and other metadata and the record containing e.g. personal data. A parallel issue exists for DRM too. There are several co-existing possibilities to organize the “Sticky policies”. There was discussion about using a binding like in XML Signature (detached and in line). There could be an online data store that contains the bindings, so the PEP could just ask there. An additional issue came up while considering that access policies with conditions travel around. The sending service has a set of policies, but also the receiving service has already a certain set of policies (endogenous policies). In practice, those policies must be combined in order to compute a concrete result on whether access can be granted, or whether the receiving service is able to accommodate the requirements from the sending

service. It became quickly clear that the combinability of policies turns into a major requirement once more complex distributed systems or ad-hoc systems are considered. There are several algorithms already available, but none of them is currently standardized. But standardization of the algorithm of combination is needed to design policies and systems with predictable results. XACML currently provides a built in set of policy combining algorithms, but work is need to determine their suitability for this application.

Further work was taken up by the PrimeLife partners. As TC XACML had just finished XACML 3.0 there was no opportunity to have XACML aligned with all the ideas out of the PrimeLife project, mainly the PPL language. Coordinating via PrimCluster input papers were written to TC XACML to nevertheless achieve some impact. This included not only additions to XACML, but also added the possibility to express predicates over attributes in SAML assertions.

3.2 Workshop on Privacy for Advanced Web APIs, London 2010[4]

As the Web advances toward becoming an application development platform that addresses needs previously met by native applications, work proceeds on APIs to access information that was previously not available to Web developers. Work on Web Applications[5] and on the Geolocation API[6] for web sites triggered intensive privacy discussions. Device APIs[7] will provide broad availability of possibly sensitive data collected through location sensors and other facilities in a Web browser is just one example of the broad new privacy challenges that the Web faces today. The privacy discussion was also brought into PrimeLife for further consideration and to think about possible solutions. The dialogue was further broadened by PrivacyOS where several stakeholders had first discussions[8]. All this together let to the Workshop on Privacy for Advanced Web APIs[9] to discuss the current work on the user facing side within a broader audience. The workshop was a first step. It was the first time that browser vendors came together to talk about Privacy issues and to think about possible solutions, especially for the APIs that would convey data to third parties. How would one protect the API that can query data in the device owner's address book to ease the sharing of such information e.g. at a business meeting? How could the system distinguish between desirable functionality and undesired spying or data leakage?

Consequently, the workshop on Privacy for Advanced Web APIs served to review experiences from recent design and deployment work on APIs at W3C, and to investigate novel strategies toward better privacy protection on the Web that are effective and lead to benefits in the near term. W3C Geolocation Working Group, the W3C Device API and their security and privacy considerations were under scrutiny and PrimeLife results were presented as possible remedies. New Appstores appear on different platforms with applications for our mobile devices. Web applications use Web technology to provide such applications for desktop and mobile devices. So questions from the Web Applications Working Group were getting even more emphasis by the

4 http://www.w3.org/2010/api-privacy-ws/
5 http://www.w3.org/2008/webapps/
6 http://www.w3.org/TR/geolocation-API/
7 http://www.w3.org/2009/dap/
8 https://www.privacyos.eu/
9 http://www.w3.org/2010/api-privacy-ws/

W3C Technical Architecture Group's recent and future work on a Web Application Architecture including the Privacy challenges, unanswered so far.

PrimeLife came just in time to help organize this important Workshop and also use it to distribute some if its results. It also influenced the choice of the topics as usability is high on the agenda of the browser vendors and PrimeLife had something to say on that. The Workshop was hosted by Vodafone in London. It brought together the top players of the browser world and worldwide research and user communities.

Major initiatives were presented and their privacy aspects discussed. Hannes Tschofenig (Nokia Siemens Networks and Internet Architecture Board) discussed the privacy philosophy commonly used in the IETF's standards work (slides), characterized as a hybrid of "privacy by design" and "privacy by policy." He noted that different approaches relate to different communities, with the first for engineers, the second for policy makers. He called out education and awareness building; guidelines for privacy-friendly protocol design; review; privacy-related coordination among standards bodies; agreements on terminology as concrete steps that could be taken by standards organizations. It was noted in the discussion that by raising privacy to the user, especially with too many dialogs, it is possible to "spook the users" and reduce the benefit of new services and technologies, yet there are risks (such as combining "my location" with known aspects of various locations).

The workshop on Privacy and Advanced API's was oriented towards concrete advancements and real world challenges. An economic analysis of Privacy and data collection dynamics was presented and found a lot of echo with the participants as it explained one of the most important inhibitors for privacy on the Web. It revealed that differences in data collection alone did not make test subjects prefer one online vendor. Their decisions were dominated by the economic factor, even against their stated preferences.

In addition to technical and user interface challenges, there were questions about the business incentives for browser vendors and large Web providers, as one of the main obstacles for getting privacy from research and standardization to deployment. Nevertheless, further investigation and experimentation with both approaches seems worthwhile and was encouraged.

The two practical proposals that drew most interest and discussions were the Mozilla privacy icon approach[10] and CDT's privacy rule-set idea[11]. Both proposals received a lot of positive feedback, and questions about their viability. In addition to technical and user interface challenges, there were questions about the business incentives for browser vendors and large Web providers, as one of the main obstacles for getting privacy from research and standardization to deployment. Nevertheless, further investigation and experimentation with both approaches seems worthwhile and was encouraged.

There was agreement that it is useful to capture best current practices gained during early implementation efforts (such as those presented during the workshop regarding the geolocation API). Furthermore, investigating how to help specification writers and implementers to systematically analyze privacy characteristics in W3C specifications was seen as a worthwhile effort. To this end, the W3C staff plans to propose a charter for a Privacy Interest Group that can

10 http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-22.txt

11 http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html

serve as a forum for this work. Such an Interest Group could also provide a focal point for privacy-related coordination with other interested standard development organizations.

The wealth of discussions and the enthusiasm of the participants of the Workshop encouraged people to continue the dialog in a mailing list and possible future Workshops. This mailing-list has gained more and more momentum with participants from both sides of the Atlantic and is the basis for the building of a true privacy community for the Web.

3.3 W3C Workshop on Privacy and data usage control, Boston 2010[12]

While the London Workshop created a community willing to really address the technical challenges of privacy in the Web context and while they started to have lively discussions on a W3C hosted mailing-list[13] the ideas about what to do are clearly not shaped yet. W3C organized a further Workshop on Privacy and data usage control[14] to encourage further discussions on the question of data usage once data has been collected. This again involved requirements and expectations from the Device API community as DAP was looking for solutions on reliable privacy friendly data handling. Earlier works in the PRIME project[15] and in the TAMI project of MIT[16] already tried solutions in this space. The challenge is to generate user trust by creating systems that reliably implement the promises made between the parties at data collection time.

As a complement to the considerations on access control and also as a complement to the considerations around APIs and the new challenges for Web user agents they bring, there are also considerations concerning backend services like clouds, the intra-enterprise IT landscape and data flows that cross enterprise borders. Service side operations raise privacy questions beyond mere database design. How would a service make sure that data is used within the boundaries of the promises that had been given to the user. And maintain the boundaries even if third party services are used to fulfill the user's need. It becomes immediately clear that the service side of things also has large implications for the user agent part of the equation. As a consequence, the Device API Working Group presented their list of requirements for privacy and looked for possible solutions.

The workshop revealed that the complexity presented by PrimeLife to the audience was not really an issue for the service oriented businesses that typically are handling large amounts of data within complex systems. It was also clear that extending the complex system to the user side of things and to user agents would not work either. What could work is a set of simple semantics in the dialog with the user and his user agent and only use the full complexity of solutions within or between privacy enhanced services.

It became also clear that there is still a lot of education and communication needed. Developers and also parts of the software industry determining protocols and capabilities are still not sufficiently aware of fundamental insights and goals of privacy. The translation of high level privacy goals that has last been done in the 1980ies with the OECD Guidelines and the decision of

12 http://www.w3.org/2010/policy-ws/
13 http://lists.w3.org/Archives/Public/public-privacy/
14 http://www.w3.org/2010/policy-ws/
15 https://www.prime-project.eu/
16 http://dig.csail.mit.edu/TAMI/

the German Federal Constitutional Court and also subsequently with the Directive 95/34EC on Data Protection into concrete and tangible hints and advises for software development on the Internet and on the Web is still missing. We do not really understand yet what the information revolution of the past 20 years have brought. We only start to realize that the old system of self determination that ends in a bean counting exercise isn't what will help create technical remedies for our every day life on the Web. So a new effort of translation is needed. This means philosophers, technicians and lawyers have to reconvene in discussions on what the threats really are, what goals can be set and achieved. This suggests further interdisciplinary Workshops.

During the workshop, economy of privacy was called out as a topic that would need further attention. On the Web, personal data is a currency and privacy protection is swimming against the stream of the billions earned by targeted advertisement. What framework will be need to encourage investment into privacy tools rather than into lucrative tracking tools that augment the return per served ad. The PRIME project laid the theoretical foundations of a complex data handling system obeying to Privacy rules. Some people compared it to DRM for Privacy. Within a system that is 100% under control of one single entity, the implementation of such a system is burdensome but feasible with reasonable effort. But as soon as information has to travel cross boundaries of enterprises or other institutions, things become even more complex. This complexity can be handled, but would need substantial investment into Privacy enhancements of the system. But currently, most stakeholders on the web don't see a data handling solution that would be economically viable unless it is part of a larger branding strategy. Jacques Bus suggested that liability rules would give such economic incentives to invest further in systems that could control data handling, data mining and data warehousing and that would help to avoid making mistakes with consumer data.

3.4 The Internet Privacy Workshop with the Internet Architecture Board (IETF)[17]

In December 2010, W3C, with the help of PrimeLife, co-organized a workshop with the Internet Architecture Board. The Workshop will served to broaden up the privacy-question from the Web to the Internet at large. Raising the topic was initially triggered by the London Workshop and the increased dialog on Privacy between W3C and the IETF that was made possible by the PrimeLife/W3C workshops and the continued monitoring of the topic by the PLING (Policy Languages Interest Group) Topic and tone were much more general and also rather oriented towards protocols.

This workshop explored conflicting goals of openness, privacy, economics, and security to identify a path forward within their representative organizations that could improve privacy.

There was an agreement to work together in a number of areas within the broader Internet technical communities such the IAB, W3C, and Internet Engineering Task Force(IETF). This means that the IETF and W3C will intensify their dialog on Privacy to give it more consideration than in the past. They will try to further organize and shepherd the debate around Internet Privacy.

One of the main echos during the workshop was related to “Privacy by design”, a topic already explored at the workshop on Privacy and data usage control. While the earlier workshop tried to

17 http://www.iab.org/about/workshops/privacy/2010-privacy-workshop-press-release.pdf

find a technical answer to that question by making data easy to handle with the help of a metadata or labeling system, the IETF workshop took a different view.

In the IETF, there is a long tradition to require security considerations[18] for every RFC[19]. This requirement had been hardened by RFC 3552[20]. During the workshop there was a lot of promotion to add an RFC that would force authors of RFCs or W3C Recommendations to include a mandatory section on Privacy considerations thus forcing the designers of technology to take Privacy into account and to justify if the technology has privacy-invasive characteristics. This will be further pursued and will take some time. Currently there is no Internet-Draft (first step) suggesting such a mandatory section.

3.5 Workshop on Web Tracking and User Privacy, 28/29 April 2011, Princeton, NJ, USA

Partner W3C got involved into the larger US debate on new measures to protect the Privacy of citizens as they were asked to comment[21] on the Notice of Inquiry on Information Privacy and Innovation in the Internet Economy by the US Department of Commerce[22]. The discussion about online tracking (for example for behavioural advertising) and possible countermeasures has picked up a lot of momentum, fueld addtionally by the Privacy Report from the US Federal Trade Commission[23].

Several vendors are offering measures that are intended to permit users to opt out of this tracking, or to prevent tracking by Web sites that are known to engage in these practices. For example:

- Microsoft announced the inclusion of anti-tracking technology based on tracking protection lists in IE9. This technology was submitted to W3C (see staff comment[24]).
- Mozilla announced support for a "do not track" header[25].
- Google announced a browser extension that permits users to persist opt-out cookies[26].

Similar technology is already deployed in a number of plugins for various browsers, including, for example, NoScript, AdBlock plus, TACO, and PrivacyChoice. The workshop was intended to establish a common view on possible standardisation work in the Web privacy and tracking protection space. There were further negotiations and discussions with the IETF who had similar works contributed to the IETF Prague meeting.

With almost hundred participants present, the workshop attracted a broad set of stakeholders, including all major web technology providers, smaller technology providers, privacy advocates

18 http://datatracker.ietf.org/doc/rfc2223/?include_text=1
19 Request for Comment, the name of IETF specifications
20 http://datatracker.ietf.org/doc/rfc3552/?include_text=1
21 http://www.w3.org/2010/06/DoC-NoI-privacy.html
22 http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf
23 http://www.ftc.gov/opa/2010/12/privacyreport.shtm
24 http://www.w3.org/Submission/2011/01/Comment/
25 http://firstpersoncookie.wordpress.com/2011/01/23/more-choice-and-control-over-online-tracking/
26 http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html

and governmental representatives from the US and the EU. This included implementers from the mobile and desktop space, large and small content delivery providers, advertisement networks, search engines, policy and privacy experts, experts in consumer protection, and other parties with an interest in Web tracking technologies.

Discussion focused most on the meaning, implementation and enforcement of an expressed Do Not Track preference, though Tracking Protection Lists and other mechanisms were also debated.

Among the diverse group of participants few points went uncontested. Nonetheless, some areas of consensus emerged:

- Regarding the applicable definition of tracking, there were no show-stopping objections to a broad definition of tracking with exceptions for certain common practices.
- Participants agreed that time was of the essence in moving forward with standardization of Do Not Track preference expression technology.
- There was general support for an Interest Group in the W3C to consider privacy issues on the Web on an ongoing basis.

The chairs have concluded that the W3C should pursue chartering a general Interest Group to consider ongoing privacy issues and a Working Group to standardize technologies and explore policy definitions of tracking.

3.5.1 Goals and Scope

Workshop participants first considered the goals of tracking protection and the scope that Do Not Track (DNT) and other mechanisms should cover, a theme that would recur throughout the two days. Presented research on user expectations of tracking and "Do Not Track" (Aleecia McDonald presented compelling data, with hopefully more to come from CMU) showed a disconnect between users' understanding and both the current state of technology and proposed mechanisms for tracking protection. Discussion highlighted the challenge of educating users about ongoing tracking and providing transparency and control.

The second set of panelists debated what should or should not qualify as tracking that users should be able to opt out of. Francis Larkin of Facebook argued for parties with existing relationships with the user (as in the case of social widgets and the Facebook "Like" button) to be exempt. Andy Steingruebl of PayPal emphasized the need for detailed logging for the purpose of fraud prevention. MeMe Jacobs Rasmussen of Adobe also brought up the issue of 1st vs. 3rd parties, arguing that 3rd parties contracted to collect data for 1st party purposes (as in analytics) should be understood as 1st parties to the user. In discussion of each of these cases, the question of user expectations loomed large: which existing tracking practices do (or should) users expect, understand and appreciate?

3.5.2 Mechanisms

Alex Fowler explained the reasoning behind, and some preliminary results from, implementing the Do Not Track HTTP header in Firefox 4. He emphasized not taking an anti-advertising stance and enabling communication between the advertiser and the end user. Fowler was also able to report

on some implementation experience: 30 lines of code for implementation in Firefox 4, and at least the Associated Press and Chitika have started to recognize the header on the server side. Adrian Bateman presented the reasoning behind Microsoft's Tracking Protection Lists, emphasizing balance, choice (including an ecosystem of different blocking lists) and innovation. Jonathan Mayer argued against the necessity of a DOM equivalent to the DNT HTTP header. John Morris responded to some common past arguments against user privacy preference expression technologies (lack of self-enforcement; difficult UI; blaming the browser; false sense of security; no certain success) in support of a Do Not Track expression mechanism and potentially similar future mechanisms.

Multiple participants (from BlueKai, Datran Media and Yahoo!) argued for a mechanism that would interoperate with behavioral advertising self-regulatory programs and allow for communication between the site and the user about why tracking was happening and its economic consequences.

Finally, the workshop group discussed several issues of granularity. Frederick Hirsch discussed DAP's work on representing more than just binary preferences (as in Privacy Rulesets) as something to consider in defining a wire format. Harlan Yu discussed the possibility of an HTTP response header as an "ack" from the server that the preference was received and either followed or not, which inspired some debate about whether such a response would make compliance and enforcement easier or more difficult.

3.5.3 User Experience

Friday morning's first panel, starting with Ian Fette from the Google Chrome team, emphasized the importance of the user experience and user interface to any privacy-preserving technology in this area. Serge Egelman (NIST) discussed the importance of empirical research for developing user interfaces and user interface design patterns that help users understand the implications of their actions: like showing sample details rather than just high-level categories in permissions interfaces. Yang Wang from CMU proposed an empirical study comparing different Do Not Track tools and interfaces and how users understand them.

In discussing standardization of user experience, a common view was that it was difficult or even counter-productive to standardize the user interface. Nevertheless, there was advice that thinking about the implementation of UI and UX in a working group would be valuable: Lorrie Cranor reported that some implementations of P3P had copied and pasted text from the spec that had not been intended for end-user consumption and so guidelines on interface implementation would be helpful. Bryan Sullivan (AT&T) pointed the group to work done at WAC and the DAP WG on defining permissions that users may accept.

3.5.4 Compliance

Panels included discussion of both self-regulatory and regulatory compliance. Regarding self-regulation, Jules Polonetsky argued that because opt-out rates may be very small (compared, say, to the number of users that delete cookies) advertising businesses shouldn't fear a usable opt-out technology. Kevin Trilli from TrustE and Andy Kahl from Evidon, despite being market

competitors, agreed on the importance of standardization and transparency in order to confirm to users when and how their data is being used.

One substantial question was whether a Do Not Track preference would opt-out of some collection practices in addition to opting out of use for behavioral advertising. Jonathan Mayer and Aleecia McDonald argued that users would be just as upset with their data still being collected after applying Do Not Track, while Polonetsky argued that collection of data for measurement of advertising was especially important to advertising and that prohibiting all collection would for that reason scare many in the industry. Kenya Chow and Nicholas Petersen from the Samuelson Law, Technology and Public Policy Clinic highlighted the dangers of "weasel words" or vague exceptions in self-regulatory language that could allow almost anything.

Ed Felten presented an overview of FTC's role and interest in Do Not Track, including the five desired properties of such a mechanism:

1. Is it universal? Would it cover all trackers?
2. Is it usable?
3. Is it permanent? Does the opt-out expire?
4. Does it cover all tracking technologies?
5. Does it cover collection in addition to use?

The FTC has not yet taken a position on whether legislation is necessary, but Felten concluded that the FTC would be happy if multiple stakeholders came to an agreement on Do Not Track. Concerning self-regulation, the FTC might be one venue to receive reports of violations of a self-regulatory code of conduct.

Chris Soghoian, formerly of the FTC, presented thoughts on potential security/fraud exceptions to DNT, arguing that in many cases fraud protection would mostly be covered by first-party interactions (like clicking on an ad) rather than third-party tracking across multiple Web sites. Soghoian argued that DNT should provide stronger protections than simply blocking third-party cookies in the way that Apple's browsers do by default. There was some debate over what level of collection or retention was necessary for impression fraud protection. Andrew Patrick from the Canadian Office of the Privacy Commissioner provided the provocative slide that current Web tracking was breaking the law in Canada and argued against letting trackers off the hook too easily. Rob van Eijk from the Dutch Data Protection Authority provided input on a potential new EU privacy directive and its relation to Web tracking.

3.5.5 Standardization

Sue Glueck of Microsoft introduced standardization by polling the audience on how many technical people (lots) have been involved in policy issues within a technical standards body (many fewer). Glueck also asked whether the IETF's scope included this sort of policy work. Alex Fowler from Mozilla identified finding consensus, defining outcomes and enabling enforceability as advantages of standardization and proposed that standardization could be divided between IETF (HTTP DNT header and response) and W3C (TPLs and DNT DOM property). Fowler argued that the group of participants had the necessary expertise, but lacked the full range of necessary stakeholders including display advertising, for example, and offered that he could help contact those parties. Peter Saint-Andre gave an explanation of IETF's very open process based on rough consensus and running code and highlighted the similarities between IETF and W3C (including

the people involved) and their positive relationship. Thomas Roessler (W3C) and Peter Saint-Andre (IETF) agreed that HTTP headers were an extension point that could be defined outside of IETF, potentially with IETF review.

Alex Fowler, Jonathan Mayer, John Morris and Wu Chou all suggested some kind of separation of the standardization workflow between TPLs and DNT. Vinay Goel (Yahoo!) and John Morris both suggested that defining the policy meaning of Do Not Track might best be done outside of a technical standards body. Hannes Tschofenig and Thomas Roessler gave examples of standards bodies providing guidance to government policy makers.

3.5.6 Next steps

In the final session, participants openly discussed the next steps for this process, in terms of scope, timeline and direction.

Initially, regarding definitions of tracking, two "hum" polls were taken. Among three choices for tracking — all tracking; tracking for online behavioral advertising; or some middle ground broad definition with certain exceptions (as in CDT's or EFF's proposals) — participants were fairly evenly divided on which proposal they would prefer to start with. Among the same set of choices, participants were also asked which would be a non-starter: while there were objections to the broad definition and the OBA-only definition, no one responded that the CDT-style proposal was an unacceptable starting point.

There was general agreement that, given the level of interest, work needed to progress quickly, but there was disagreement on whether preliminary work needed to be done in weeks or months. Ashkan Soltani and Alissa Cooper made the point that the feasible length of the timeline depends on the breadth of the scope: a narrower technical proposal could be completed more quickly while a larger policy agreement would take longer.

It was suggested that a Do Not Track proposal needed to be completed very quickly in order to take advantage of the current US legislative session (Alissa Cooper and others), and also a concern that the window of legislative focus was narrow (one shot only for the next several years) and so proposals should be completely defined. There was some debate over whether a "beta" definition of tracking would be valuable (to have something done quickly and to guide existing implementations) or harmful (in changing underneath implementations).

Thomas Roessler emphasized the importance of developing a world-wide solution, given the relevant ongoing debate in Europe and other regions.

Karl Dubost (Opera) suggested that an Incubator Group could be formed to document existing work and definitions and decide on next steps and Bryan Sullivan thought a landscape document would be a good first step. There was pushback, however, on only developing an Incubator Group given time pressures and intensity of interest.

There was broad support, suggested by David Singer and echoed by others, for an Interest Group to consider privacy problems on an ongoing basis and spawn specific projects as necessary.

3.6 Workshop on Identity in the Browser 24-25 May 2011, Mountain View (USA)[27]

As the Web becomes increasingly a focal point for economic and social activity, there is an urgent need for trustworthy, widely-applicable digital identity management. This includes the need for authentication and authorization to work across multiple web-sites, enterprises, devices, and browsers in a uniform and easy-to-use manner. For critical enterprise activity, effective government engagement, and sensitive social information accessed over the Web, a higher level of identity assurance, privacy protection, and security is required beyond simple username/password combinations. To address many of these issues, digital identity should become a core part of Web architecture, enabled by a combination of server and client-side solutions. Achieving this vision, however, requires addressing numerous technical, operational, policy, and legal issues. This workshop's purpose is to consider how the intersection of those issues with the use of browser technology can lead to this vision.

Many approaches to managing digital identity, such as SAML and OpenID, have been deployed without requiring special-purpose technology on the browser client. There is, however, a general understanding within the technical community that client-side mechanisms working together with the server will improve usability, security, and trust. Ideally, effective identity authentication and authorization shouldn't be tied to a single browser, but be capable of being switched across multiple devices such as phones and desktops in a privacy-respecting manner. At the same time, it would need to provide a level of assurance high enough to be suitable for use in financial, healthcare, and government-grade applications. Implementing digital identity technologies of this sort is an effort that crosses the boundary between server and client. Rather than starting from a blank slate, any new work should compliment existing technologies while enhancing usability, privacy, and security.

Currently, the workshop has 54 position papers from major industry stakeholders and from research. Hopefully, there will be some agreement to have an integrative approach that would include higher security governmental ID-systems as well as privacy enhancing features.

3.7 The Federated Social Web Summit Europe 2011

The Social Web is a set of relationships that link together people over the Web. While the best known current social networking sites on the Web limit themselves to relationships between people with accounts on a single site, the Social Web should extend across the entire Web. Just as people can call each other no matter which telephone provider they belong to, just as email allows people to send messages to each other irrespective of their e-mail provider, and just as the Web allows links to any website, so the Social Web should allow people to create networks of relationships across the entire Web, while giving people the ability to control their own privacy and data. The standards that enable this should be open and royalty-free. We present a framework for understanding the Social Web and the relevant standards (from both within and outside the

27 http://www.w3.org/2011/identity-ws/

W3C) in this report, and conclude by proposing a strategy for making the Social Web a "first-class citizen" of the Web.

Diverse social networking sites could federate using inter-operable standards to share social data like status updates. To make this vision a reality on a truly large-scale, more work on standardization, policy, test cases, and more experimentation and experience with actual deployment and code are needed. Good identity management is key to such an interoperable and scalable social web. But identity-management may be very privacy invasive and high anonymity may lead to irresponsible behaviour. The right balance for trust remains to be found. The workshop also contributes to this debate.

The new requirements will be discussed, as increasingly users must further be able to trust the Social Web to allow them to communicate securely with their peers and have their privacy respected. Both legal policy-based approaches to the handling of personal information related to social networking and strong cryptographic technology can be leveraged to improve the current state of the art in decentralized social network services. In the long-run, our society will be more and more dependent on the exchanges done via social networking services, so architectures and standards for the Social Web should therefore be designed to be robust and resilient against attack.

The workshop aims to capture, discuss and address the challenges and the potential of innovations in the federated social network space. The workshop will kick off with talks and panels on Friday June 3rd, to be followed by discussion of position papers about possible future standards and architectures. Afterwards, an open space will begin on Saturday June 4th and early Sunday June 5th, to enable further discussion, collaborative coding, development and experimentation.

This workshop intends to bring together communities building federated social networking code-bases with those involved in privacy and identity. It will be the second conference, following up on the original Federated Social Web Summit in Portland in 2010, but now with a focus on privacy protection in the social web and the cloud. As it is a W3C Workshop, it will have one day for position papers and discussion. To continue the tradition of the Federated Social Web Summit in Portland in 2010 and attract more developers, the summit will also have a open-space, including opportunities for collaborative coding and open talks, for an entire day.

Chapter 4

Standardisation coordination and contribution

While the workshops had mainly an exploratory purpose, they nevertheless triggered concrete contributions to standardisation works. PrimeLife itself did not trigger any standardisation directly and exclusively tied to its work as described in Annex1. This is a good sign as PrimeLife was oriented towards influencing current work under way to make it more Privacy-friendly and also geared towards practical Privacy improvements for citizens and companies. That meant for PrimeLife to integrate into the current technical platforms that are Web, Internet and Mobile.

Looking at the concrete textual contributions does not reveal the enormous efforts put into coordination of various efforts in order to funnel them towards communities where they would have the highest impact. Bringing the Privacy community technically closer together to achieve a higher impact in standardisation and elsewhere will never be an easy task. PrimeLife has achieved much here, but not all of it will be measurable or visible. The measurable and visible parts are listed below.

4.1 PrimCluster

PrimeLife is not the only research project focusing on Privacy. Because it is a complex topic, Privacy is not an easy sell in technology and ICT. Together with their European Commission's project officers, several projects decided to pool their resources in standardisation together to get a higher momentum. The coordination was called “PrimCluster”. PRIMCluster was used as a platform to help coordinating standardisation investments with other projects to reach critical mass triggering sufficient attention by standardisation bodies. Participants were SWIFTS, TAS3, PICOS, PrimeLife, EnCoRe, Turbine, MASTER and Think-Trust.

PrimCluster served as a coordination point with the NESSI standardisation working group and the Software & Services area of the EC. Further coordination was done with the TAMI project at MIT, which addressed similar issues.

PrimeLife not only helped the other projects with their standardisation strategy, but also benefited from the momentum provided by the other projects for their own initiatives. All workshop of 2009 and 2010 had participation from representatives of other partners of the PrimCluster coordination. The concerted actions out of the workshops were instrumental in getting standards bodies attention. The offered contributions had sufficient weight behind them to have an impact in standardisation, at least as far as XACML goes, but also beyond.

Despite the fact that some of the projects within the PRIMCluster have ended, the initiative was again successfully utilized to create momentum for the second and the third PrimeLife Workshop in cooperation with W3C. On 10 September 2010, all projects of PRIMCluster met to discuss common strategies towards data handling and obligations that go beyond access control. A coordination of submissions towards the planned PrimeLife & W3C Workshop on Privacy and data usage control was achieved.

4.2 ETSI

PrimCluster served as a coordination point for the ETSI standardisation on an ISG on Identity and access management for Networks and Services. The ISG targets specifications for the application of identity and access management to networks and services. One aspect is the definition of requirements, scenarios and use cases. A central part is the development of appropriate architectures to link various silos of existing Identity management systems and provide mechanisms to bridge the gap in the integration within existing telecommunications infrastructure. Furthermore, specifications of protocols and APIs, as well as profiles of existing standards are in the scope of the ISG.

4.3 OASIS

The first workshop on Access Control Application Scenarios laid the groundwork for the relation to OASIS. Data protection is a big consumer of access control technologies. PrimeLife has a focus on XACML. W3C was able to draw the attention of the chair of TC XACML to the workshop and was able to engage him as a chair. OASIS, by its structure and lack of technical staff is less capable of organizing such workshops. But OASIS is a member of W3C, so cooperation was just smooth. The workshop report indicated the need for further coordination efforts. The goal of Primelife was to include the special attributes for anonymous credentials into XACML and to push for further privacy enhancements. These contributions and submissions to TC XACML are currently in progress. At the third Workshop on Privacy and data usage control in Boston further steps have been negotiated with the Chair of TC XACML. The contribution of the attributes specification was agreed and a timing set. TC XACML is also instrumental in helping to coordinate the additional profile specifications for the SAML (Security Assertion Markup Language) extensions that would allow the use of selected and potential anonymous credentials in the XACML/SAML environment and thus bring this technologies to the web services world.

4.4 DIN

PrimeLife participated in a Focus ICT group of DIN helping to shape the perspectives of privacy standardization in 2010. Partner ULD and W3C participated together in seminars of the focus group and chaired sessions. Insight and knowledge gathered by PrimeLife served to enlighten the participants from DIN and ISO to get an idea how the Privacy problems in smart metering, road tolling and smart houses. DIN considered PrimeLife contributions so essential that they renewed the exact set up in 2011 with contributions from partners ULD and W3C. This was mostly cost neutral for the project as DIN was paying travel expenses.

4.5 IETF

Apart from increasing discussions among IETF experts and PrimeLife partners, the project's results have been picked up in two early internet drafts:

"Privacy Preferences for E-Mail Messages,"[28] i.e., the icon set "Privicons" that aims at communicating the sender's preferences for handling an e-mail to the recipients (cf. Section 15.6) and

- "Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management."[29] that is based on "A terminology for talking about privacy by data minimization" [30].

It remains to be seen how these documents will evolve and whether ideas from these drafts will affect internet standardisation at a later stage.

4.6 Global Platform[31]

For the implementation of the mobile demonstrator, G & D used the Global Platform as a venue. G & D is a full member of Global Platform. No other PrimeLife partner is member of the Global Platform. The mobile demonstrator for PrimeLife is using Secure Elements (SEs). Those are platforms, particularly for Mobile Devices, on which Applications can be installed, personalised and managed. Increasingly, this can be done over-the-air (OTA). OTA provisioning of Applications is done via a Trusted Service Manager (TSM). This helps to adapt formerly static SEs more flexibly for new Mobile Services and Applications.
The appeal of SEs will be particularly high to the respective service providers if they rapidly, easily and seamlessly integrate with applications provided by Third Parties in the market place. Quick diffusion can be expected, if the Secure Elements in the Front-End enable these Third Parties to embed security, privacy and identity-management into their solutions ad hoc. Further, a

28 http://tools.ietf.org/html/draft-koenig-privicons

29 http://tools.ietf.org/html/draft-hansen-privacy-terminology

30 Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management v. 0.34. https://dud.inf.tu-dresden.de/Anon Terminology.shtml, August 2010.

31 http://www.globalplatform.org/specificationsdevice.asp

pre-certification of the Secure Elements with regard to security, privacy and identity-management may still enhance market acceptance, as it would provide independent solution and application providers with a “dock-on” method to security, privacy and identity-management.

To achieve this goal, clear and open interfaces will be essential. Further, a combination of hardware, software, interfaces and protocols needs to inter-play in order to enable the secure storage and usage of credentials for increasingly sophisticated Mobile Services. For this, technologies such as the ARM TrustZone may be leveraged, because of their dominant design in the marketplace for Mobile Device platforms.

The so-called Trusted Execution Environments (TEEs) are striving to provide the above-mentioned characteristics.

In order to remain highly flexible and adaptive to changes in the environment of Mobile Services, TEEs strive for independency from the Rich-OS. This is particularly important as increasingly open Rich-OS systems diffuse in the Mobile Devices, e.g., Googles Android. Modern TEE approaches can be used on a wide range of TrustZone systems, especially if they are equipped with a clean and easy to understand integration interface. Here, reference drivers can be leveraged that help TEEs integrate with specific Operating Systems, such as Googles Android.

TEEs provide security, privacy and identity-management solutions that enable new types of services. TEEs address the need for flexible, powerful and efficient security solutions in various forms of Mobile Devices. Among others, TEEs can, for example, be based on ARM TrustZone enabled chipsets (so called SoCs). TEEs utilise ARM TrustZones division of the SoC into two distinct areas, a “Public World” and a “Private World” as shown in Figure 2.3. TEEs then provide open interfaces in order to enable the development of dedicated applications with security, privacy and identity-management capabilities.

In this concept of “Public and Private Worlds”, the TEEs encapsulate security-, privacy and identity-management-relevant parts of an application in the dedicated “Private World”. Those parts of the application that are not security-, privacy- or identity-management-relevant remain in the “Public World”. Two clear and open interfaces between the “Public” and the “Private World” – the so called TEE Client Application Protocol Interface (API) and the TEE Internal API - enable application providers to dock-on to the concept. Leveraging these two API empowers them to offer secure services to the market without having to go into the details of security and privacy protection or the specifics of identity-management.

G & D wrote a complete specification for the TEE and contributed it to Global Platform. The specification was published on 10 July 2010 and is available for download at Global Platform website[32].

32 http://www.globalplatform.org/specificationsdevice.asp

Chapter 5

ISO Standardisation

Based on its liaison PrimeLife submitted comments to CD 24760 “A framework for identity management”.

In ISO, the joint technical committee ISO/IEC JTC 1/SC 27 is in charge of standardising security standards for information systems. Among other things, they are behind the 27000 series on information security management systems. Within SC 27 the working group 5 (WG 5) is responsible for standards within the identity management and privacy area.

Early on, PrimeLife established a cooperation with WG 5 in the form of a liaison agreement with the group. The reason for the liaison is that WG 5 is working on a number of standards that have commonalities with the aims and the scope of the PrimeLife project and we wanted to be able to influence these standards and to contribute with our knowledge and findings in the standardisation process. The contributions of PrimeLife have been very well accepted by WG 5 and we believe that we have had mutual benefit from the cooperation. Even though the whole spectrum of the standards within WG 5 is of interest, there are three projects that lie close to the work going on in PrimeLife and we have therefore decided to concentrate our contributions to these standards.

The projects concerned are the 24760 “A Framework for Identity Management” standard, the 29100 “Privacy Framework” standard and the 29101 “Privacy Reference Architecture” standard. Most of the contributions have been in the form of discussions on work group meetings and comments on standard drafts; however, there are some areas where PrimeLife has made very significant impact. The remainder of the subsection will discuss specifically PrimeLife’s input to the Framework for Identity Management and the Privacy Reference Architecture.

5.1 ISO 24760 – Framework for Identity Management

ISO 24760 aims at describing a framework for identity management and defining its components. The standard presents terminology, concepts, identity life cycle and best practices within the identity management area. It started out as a monolithic standard, but after suggestions from PrimeLife and other contributors, it was divided into three parts. The biggest issue within the standard has been around terminology and the interpretations of the different terms. There were also some discussions on the format of the descriptions of the different terms. PrimeLife suggested a total make-over of the structure and format of the terminology and as a result of this, one employee at one of our partners became the co-editor of the standard.

Identity is an important and ambiguous concept in identity management. The understanding of the term (and the implications of that understanding) ranges from a collection of attributes associated with an individual to a collection of attributes making an individual unique. In the realm of natural or legal persons, it is easy to argue that an identity is a collection of attributes associated with an individual.

However, if the identity concept is pushed into the realm of objects, the understanding or the limits of the concept becomes problematic. Potentially, one could argue that one unit of data would be an identity or that everything is an identity if an identity is defined as a collection of attributes associated with an object. A consequence of this is then that every computer system is an identity management system, which is not in line with the understanding of the experts in the field and could also make the concept of identity essentially useless since nothing exists that is not an identity.

On the other hand, requiring that an identity always uniquely identifies the entity blurs the difference between identity and identifiers. More or less, this understanding makes it pointless to allow a user to have multiple identities in the system and potentially creates large privacy problems. As a consequence, one of the biggest issues regarding the terminology has been the concept of identity including terms like identifier and partial identity. The problem with partial identity is that the concept is rather new and not used that much outside of research circles.

Some of the attending experts thought that it could be hard to push it into an industrial setting even if they do agree with and understand the concept. In the terminology discussions, PrimeLife has provided its view of the concepts. PrimeLife also contributed in making the document consistent and in advocating the users' view and tried to gear the standard into a more user-centric model by providing the experience gained and discussions held during the project.

5.2 Introducing Privacy Protection Goals to ISO 29101 Privacy Reference Architecture

IT security[33] and privacy protection are overlapping perspectives when implementing IT systems. They both need to be considered already at the level of developing underlying architectures.

33 Note that we use the term "IT security" in its broad meaning of "information security" covering all security aspects of the full information system, regardless, whether technological components are involved or not. Among others, organisational processes, data on all kinds of media or the staff involved in data processing are part of this comprehensive approach, e.g., when analysing risks or selecting and implementing appropriate countermeasures.

Usually, IT security takes the perspective of an organisation, i.e. the objective is to safeguard the assets of that organisation. Here the "Classic CIA Triad"[34] of the IT security protection goals (confidentiality, integrity and availability) is applied as necessary for the specific context. These protection goals are useful to structure risks and countermeasures, and to set up a working Information Security Management System (ISMS).

In contrast, privacy protection focuses on the individuals concerned, i.e., the Data Subjects. Certainly the IT security protection goals confidentiality, integrity and availability are important here, too, but they do not represent all areas that should be covered when it comes to the privacy of an individual as well as to the compliance with today's data protection regulation[35].

IT security protection goals such as confidentiality, integrity and availability may facilitate the implementation of privacy principles into an IT system, but do not suffice to cover all aspects of privacy protection. For privacy protection, these goals need to be complemented with a set of specific protection goals that also allow for the expression of mismatches and conflicts of different goals. Even with the three classical IT security protection goals, it always has to be determined how much each goal should be pursued and what balance between conflicting aspects of those goals should be achieved. With the extension to six of those high-level protection goals, potential conflicts are more visible, which is good because they have to be tackled when designing, operating and improving the IT systems. There is no "one size fits all" solution, but for each application context, individual balances and implementations have to be determined, dependent on, e.g., the sensitivity of data, the attacker model, legacy issues from already existing components of the information system, and last but not least, legal obligations.

To allow for a more holistic mapping of privacy principles, the three IT security protection goals are supplemented by three privacy-specific protection goals: transparency, unlinkability and intervenability, as explained below. A hexagon of protection goals can be derived where each goal is countered with another one expressing dualistic aspects of the protection, see Fig. 25.1[36] . All protection goals can in principle be applied both on the information itself, as well as on the processes, and technical layers. For each, the perspective of the Data Controller, the Data Subject and a third party can be adopted. Privacy protection goals help to structure risks and to define which measurements to apply.

34 CIA stands for Confidentiality, Integrity and Availability, not for the well-known secret service.

35 Martin Rost and Andreas Pfitzmann. Datenschutz-Schutzziele - revisited. Datenschutz und Datensicherheit (DuD), 33:353–358, 2009.

Martin Rost and Kirsten Bock. Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen. Datenschutz und Datensicherheit (DuD), a 35(1):30–35, January 2011.

36 See footnote 35

Fig.1 Segments of security and privacy protection goals

To support and develop a common understanding of the aforementioned concepts that could only be addressed briefly herein, the terms and definitions above have been submitted as a comment from PrimeLife to the drafting of ISO 29101 Privacy Reference Architecture.

In the following, the privacy-specific protection goals are explained:

Transparency: For all parties involved in privacy-relevant data processing (specifically the Data Controller, Data Processor(s), Data Subjects as well as supervisory authorities), it is necessary that they are able to comprehend the legal, technical, and organisational conditions setting the scope for this processing. Examples for such a setting could be the comprehensibility of regulatory measures such as laws, contracts, or privacy policies, as well as the comprehensibility of used technologies, of organisational processes and responsibilities, of the data flow, data location, ways of transmission, further data recipients, and of potential risks to privacy. All these parties should know the risks and have sufficient information on potential countermeasures as well as on their usage and their limitations.

Transparency is a necessity for important aspects of informational self-determination, such as access rights, informed consent and notification obligations of data processors. It can be achieved or enhanced by several mechanisms, such as documentation, logging, reporting, data protection management systems as well as information of and communication with the Data Subject.

Unlinkability: Unlinkability means that all privacy-relevant data processing is operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy-relevant data outside of the domain (or the applicability of a well defined purpose), or at least that the implementation of such linking would require disproportionate efforts for the entity establishing such linkage.

Unlinkability is the key element for data minimisation as well as purpose binding. Its objective is to minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling spanning across contexts and potentially violating the purpose limitations related to the data.

Wherever feasible, Data Controllers, Data Processors, and system developers should completely avoid or minimise as far as possible the use and possibilities for linkage of privacy-relevant data, conceivably by employing methods for keeping persons anonymous, for rendering persons anonymous ("anonymisation"), or for aliasing ("pseudonymisation"). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If privacy-relevant data cannot be avoided, they should be erased as early as possible.

Intervenability: Intervenability aims at the provision of possibilities for Data Subjects, Data Controllers as well as supervisory authorities to intervene in all kinds of privacy-relevant data processing, where necessary. The objective is to offer corrective measures and counterbalances in processes. For Data Subjects, intervenability comprises the Data Subject rights to rectification and erasure or the right to file a claim or to raise a dispute in order to achieve remedy when undesired effects have occurred. For Data Controllers, intervenability allows them to have efficient means to control their Data Processors as well as the respective IT systems to prevent undesired effects. Examples for such means may be the ability to stop a running process to avoid further harm or allow investigation, to ensure secure erasure of data including data items stored on backup media, and manually overruling of automated decisions or applying breaking glass policies. For supervisory authorities, intervenability could consist of ordering the blocking, erasure or destruction of data, or in severe cases stopping the data processing entirely.

Intervenability can be achieved or supported by mechanisms such as the provision of a single point of contact (SPOC). Other approaches include a separation of processes, as a means to allow the system to continue to be working, even if there is the need for intervention in a specific case. The Data Subject should be offered an easy and convenient way to exercise the Data Subject rights to rectification or erasure of personal data as well as withdrawing previously given consent.