

UI Prototypes: Policy Administration and Presentation – Version 2

Editors:	Simone Fischer-Hübner, (KAU) Harald Zwingelberg, (ULD)
Reviewers:	Laurent Bussard, (EMIC) Mario Verdicchio, (UNIBG)
Identifier:	D4.3.2
Type:	Deliverable
Class:	Public (Final Version)
Date:	June 29, 2010

Abstract

Privacy Policies are an important prerequisite for user control in privacy-enhancing identity management. The transparency of privacy policies can be enhanced if users are informed about mismatches of a site's policy with the user's preferences. Investigating understandable and transparent privacy policies, a user-friendly visualisation of policy mismatches as well as simplified and usable privacy preference management “on the fly” are the objectives of the deliverable. User Interfaces for policy display and management also need to meet technical requirements by the PrimeLife Policy Language PPL.

This deliverable is first summarising the technical features and HCI (Human Computer Interaction) requirements of PPL, and is then discussing icons presenting the important aspects of privacy policies and different iterations of User Interface (UI) prototypes for policy display and preference administration.

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.

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

Disclaimer: The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright 2010 by KAU, ULD, CURE, IBM.

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	TBD
Chapter 1: Introduction	Simone Fischer-Hübner (KAU)
Chapter 2: Background	Gregory Neven (IBM)
Chapter 3: Policy Icons and Tests	Leif-Erik Holtz (ULD), Harald Zwingelberg (ULD)
Chapter 4: Multiple Steps Policy Management and Display Mockups - 2 nd Iteration Cycle	Harald Zwingelberg (ULD)
Chapter 5: Policy Management & Display Mockups – 3 rd Iteration cycle	Section 5.1: Ulrich König (ULD) Section 5.2: Staffan Gustavsson (KAU)
Chapter 6: Policy Management & Display Mockups – 4 th Iteration cycle	Tobias Pulls (KAU), Simone Fischer-Hübner (KAU)
Chapter 7: Privacy Preferences Editor	Tobias Pulls (KAU), Hans Hedbom (KAU)
Chapter 8: Conclusions	Simone Fischer-Hübner (KAU)

Simone Fischer-Hübner did several editorial changes to chapters 3-7.

Executive Summary

PrimeLife aims at developing privacy-enhancing identity management systems for technically enforcing user control and information self-determination. An important prerequisite for user control in privacy-enhancing identity management are privacy policies, which can inform users about the personal data processing practices of a services side at the time when she is requested to disclose personal data to that services side. A user can in turn state her privacy preferences defining under which conditions she would like to release what data. The user's preferences can be compared the services side's policy, so that the user can be informed in case that her privacy preferences will not be met. In practice, privacy policies are however often containing complicated legal phases, which are not easily understood by end users. Besides, defining privacy preferences is a complex and error-prone task, which requires expertise about basic privacy principles. This deliverable D4.3.2 on UI Prototypes for Policy Administration and Presentation (Version 2) by PrimeLife work package 4.3 addresses therefore the following HCI (Human Computer Interaction) research challenges: *How to make privacy policies easily understandable and transparent, and how to simplify privacy preference management for end users?*

Another objective of WP 4.3's work which is reported in this deliverable is the development of user interfaces for the PrimeLife Policy Language (PPL) engine developed by PrimeLife Activity 5. A short introduction to PPL and a list of user interface requirements derived for the PPL engine are provided by Chapter 2.

The main contributions of this deliverables, which are presented in chapters 3-7, can be summarised as follows:

For increasing transparency of privacy policies, we have developed a set of policy icons for expressing relevant policy statements in abbreviated and easily noticeable form, which is presented in chapter 3. This set advances the initial icon set, which we have presented in D4.3.1. To the best of our knowledge, we were the first who have conducted intercultural comparison user studies for policy icons and the first results of these user studies are also reported in chapter 3. Our initial work in cooperation with others on icons for email usage is reported as well.

In chapters 4 – 6, we present 2nd - 4th iterations of policy management and display mockups which we have developed following an iterative design approach of subsequent mockup prototyping, user testing and improvements. All mockups are based on a multiple layered presentation of policies as recommended by the Art. 29 Working Party and present the core policy information on the top layer (what data are requested by whom for what purposes) in form of 2-dimensional tables. For a simplified privacy preference management, our UI prototypes are based on a novel approach of allowing users to choose from a set of predefined preferences and adapt their privacy preferences “on the fly” (i.e., when a services side is requesting data from them) rather than demanding from the users to define and configure their preferences beforehand. The fourth mockup iteration is a browser-integrated approach, which specifically aims at meeting HCI requirements derived from PPL.

Chapter 7 presents first user interfaces for a Privacy Preferences editor for PPL.

Finally, Chapter 8 summarises the main results and challenges that we still intend to address in our future work.

Work reported in the deliverable is still work in progress. Final results of the work by WP 4.3 will be reported in the final HCI Research Report.

Contents

1.	Introduction	12
1.1	Motivation.....	12
1.2	Objectives and Scope.....	13
1.3	Methodology	14
1.4	Related work	14
1.5	Main Contributions	15
1.6	Terms and definitions	16
1.7	Structure of this Deliverable	16
2.	Background	18
2.1	The PrimeLife Policy Language	18
2.1.1	Basics of XACML	19
2.1.2	Credential-based extensions in PPL.....	19
2.1.3	Data handling extensions in PPL	21
2.1.4	Example policy	22
2.2	User interface requirements	26
2.2.1	Credential selection.....	26
2.2.2	Matching policy dialog	27
2.2.3	Mismatching policy dialog	27
2.2.4	Preferences editor	27
2.2.5	Policy editor	27
3.	Policy Icons and Tests	28
3.1	Introduction.....	28
3.2	Related work	28
3.3	Advancement of icon approaches in year 2	30
3.4	Update on PrimeLife icon set	33
3.5	Icon sets development after D 4.3.1.....	34
3.5.1	Icons for general usage	34
3.5.2	Icons for usage in SNS.....	39
3.6	Test results	40
3.6.1	Test results from Karlstad University	40
3.6.2	Test results from CURE.....	43
3.7	Icons for e-mail usage.....	43
3.8	Future work.....	44
4.	Multiple Steps Policy Management and Display Mockups - 2nd Iteration Cycle	46
4.1	Past approaches and lessons learned.....	46
4.1.1	Goals driving the development	46
4.1.2	The first versions of the UI-prototype	48
4.2	Multiple steps approach - year 2 prototype.....	49
4.3	User feedback on the second iteration cycle.....	55
4.3.1	Test setup and conduction.....	55
4.3.2	Test results	56
4.4	Conclusions for a third iteration	57

5.	Policy Management & Display Mockups –3rd Iteration cycle	59
5.1	Description.....	59
5.1.1	Three Step design.....	61
5.1.2	Elements of the PLC.....	65
5.2	Usability test.....	69
5.2.1	Test design.....	69
5.2.2	Test participants and execution.....	69
5.2.3	Results.....	69
5.3	Discussions and conclusions.....	73
6.	Policy Management & Display Mockups – 4th Iteration cycle	75
6.1	Introduction.....	75
6.2	Selecting Active Settings.....	76
6.3	Menu Placement.....	77
6.4	Interface Authenticity.....	78
6.5	The “Send Data?” Dialogue.....	78
7.	Privacy Preferences Editor	83
7.1	The Main Tasks of the Editor.....	83
7.2	The User Interface Design.....	83
7.3	Design Rational and Future Work.....	85
7.4	Relevant Technical Details.....	86
8.	Conclusions	87
	References	89
A.	Pre-test Questionnaire & Test Scenarios for the Policy Display and Management Mockups (2nd iteration) Tests	91
A.1	Appendix 1: Pre-test information and Task.....	91
A.1.1	Introduction.....	91
A.1.2	Your task.....	92
A.2	Appendix 2: Pre-test questionnaire.....	93
A.3	Appendix 3: Agreement.....	94
B.	Pre-test Questionnaire & Test Scenarios for the Policy Display and Management Mockups (3rd iteration) Tests	95
B.1	Test Scenarios.....	95
B.1.1	Usability Tests.....	95
B.1.2	Background to the test of today.....	95
B.2	Pre-test Questionnaire (translated from Swedish).....	96

List of Figures

Figure 1. Structure of PrimeLife Policy Language (PPL).....	18
Figure 2. PPL engine architecture.....	26
Figure 3. First UI Prototype for Policy Display and Management (prototype A).....	48
Figure 4. The alternative prototype developed by CURE (prototype B)	49
Figure 5. Step 1 Data Processing Steps.....	51
Figure 6. Step 2 Preference Management	51
Figure 7. Step 3 Payment - payment via credit card	52
Figure 8. Step 3 Payment - anonymous payment via Paysafecard.....	52
Figure 9. Step 4 - Shipping	53
Figure 10. Step 5 Marketing	54
Figure 11. Step 6 Summary and Confirmation - mismatch e-mail missing	54
Figure 12. Step 6 Summary and Confirmation - mismatch with privacy preference	55
Figure 13. Steps solution by Amazon.com	60
Figure 14. PLC tree steps solution	60
Figure 15. Step 1: Shopping Card.....	62
Figure 16. Step 2: Summary	63
Figure 17. Step 3: Confirmation	64
Figure 18. My Privacy Settings.....	65
Figure 19. Payment provider selection.....	66
Figure 20. My Data field including Matching results	66
Figure 21. My Data field with a “Privacy Settings” mismatch.....	67
Figure 22. My Data field with a “User Settings” mismatch.....	68
Figure 23. “Data to Transfer” box.....	68
Figure 24. Selecting active privacy settings menu	76

Figure 25. Bookmarks based approach	77
Figure 26. Location bar based approach	78
Figure 27. Striped location bar	78
Figure 28. The user's screen showing the send data dialog, striped location bar and location based selection approach.....	80
Figure 29. The "Send Data?" dialogue with the "exclamation mark" icon for notifying users about data requests.....	81
Figure 30. Alternative "Send Data?" dialogue with the "plus" icon for notifying users about data requests	82
Figure 31. An overview of the editor's user interface, where preferences can be set for the selected attribute	84
Figure 32. An overview of the editor's user interface, where preferences can be set for categories of attributes	85

List of Tables

Table 1. Mary Rundle's icon set	29
Table 2. Mehldau's approach	30
Table 3. Icons for general use	38
Table 4. Icons for SNS usage	40
Table 5. Icon ideas of the test persons	42
Table 6. Example Icons set for e-mail usage in pure ASCII representation	44
Table 7. Icons for e-mail usage graphical representation and colour codes (Design of this representation by Andreas M. Brændhaugen licence: cc by-nc-sa)	44

Chapter 1

Introduction

1.1 Motivation

Privacy-enhancing Identity Management systems, which we are currently developing in the PrimeLife project, can provide powerful tools for technically enforcing user control and informational self-determination. Privacy-enhancing identity management implies that users can make informed decisions about the release of personal data, the selection of credentials for proving personal properties, and about their privacy and trust policy settings. For enabling users to understand the implications of data disclosures and thus to make well-informed decisions, there is a need for user interfaces (UIs) informing them in particular about the privacy policies of their communication partners. Such user interfaces should be informative while not being perceived as intrusive, and they should be intuitive, legally compliant and trustworthy.

According to Art.10 EU Data Protection Directive 95/46/EC (DPD), a privacy policy should inform data subjects¹ at least about the identity of the data controller², the purposes for which the data are intended as well as any further information such as the categories of data and recipients concerned, her right of access to and the right to rectify her data, needed to guarantee fair personal data processing. Privacy policies whether posted on websites or contained within contractual texts often include long complicated legal statements, which are usually neither read nor understood by the end users. *Making privacy policies easily understandable and transparent* is therefore an important challenge, which is addressed by PrimeLife work package 4.3 on “User Interfaces for Policy Display and Administration”. For addressing this challenge, one emphasis of our work within work package 4.3 has been on privacy policy icons, which are supporting the display of a privacy policy through especially tailored graphical presentations of policy aspects. Gross et al. [1] have shown that the perceived clarity of a privacy policy increases positive reaction to the site and its goals. Hence, easily comprehensible and transparent privacy policies are not only a mean for enhancing user control, but can also serve the interests of the service providers.

Achieving better transparency of privacy policies is also the aim of privacy policy matching and/or policy negotiation implemented within privacy-enhancing identity management systems. In this context, users define their release policies (or so-called privacy preferences) stating the users’

¹ For a definition of “data subjects”, see section 1.6

² For a definition of “data controller”, see section 1.6

preferences regarding the disclosures of their personal data. At the services sides, a so-called data handling policy (or simply “privacy policy”) specifies how and what data are processed by the service in question. If personal data are requested from a user by a service provider, the PrimeLife user-side system can compare (“match”) the services side’s privacy policy with the user’s release policy and inform the user in case of a mismatch.

For ordinary users defining and adapting privacy preferences, in a way that they protect their privacy properly, is a complex and error-prone task which usually requires some expertise about basic legal privacy concepts and principles. In the non-electronic world no equivalent task exists, which means that ordinary users have no experiences in how to define and manage their privacy preferences. Without assistance, most users would very likely fail to define and use privacy preferences at all or could accidentally define or choose privacy preferences, which are not as privacy-friendly as the users would like them to be. As security and privacy protection are often secondary goals for ordinary computer users [2], it is indeed not realistic to assume that users will spend much time and effort on privacy configurations. Hence, another major challenge, which is also addressed by PrimeLife work package 4.3, is the *simplification of privacy preference (release policy) management for end users*.

For achieving this, our approach within WP 4.3 has been to provide options of predefined “standard” privacy preferences, from which a user can choose and which she can customize “on the fly”. If for example a services side requests more data for a service than permitted by the user’s current privacy preferences and the user agrees to it, the user will at the same time be asked whether she wants to adapt her preferences and possibly save them under a new name or whether she rather wants to overrule her preference only for this single event. The set of predefined privacy preferences should represent the users’ privacy interests and thus also includes the most privacy-friendly options for acting anonymously or for releasing as little information as needed for a certain service. For more advanced users, a preference editor is provided, which allows them in a user-friendly way to configure their individual privacy preferences.

1.2 Objectives and Scope

In D4.3.1, which was the Version 1 on “UI prototypes: Policy administration and presentation”, we have presented and discussed initial UI prototypes and UI components (including the initial policy icons set) produced by PrimeLife WP 4.3, which aim at addressing the HCI challenges mentioned above, namely the challenges of providing user-friendly privacy policy displays and release policy (privacy preference) management to end users.

In this Deliverable D4.3.2, which is the second version on “UI prototypes: Policy administration and presentation”, we report on the follow-up research and development work of WP 4.3 and the progress that we achieved during the last project year on user interfaces for user-friendly privacy policy displays and policy administration. Within the last year, we have in particular refined and tested the policy icon set, and have developed three further mockup iterations, from which the first two iterations were evaluated with small guided user tests. Besides, there has also been close cooperation with PrimeLife Activity 5 on technical policy requirements and functionalities of the PrimeLife Policy Language (PPL) that need to be supported by the policy user interfaces, which are also summarised in section 2.2 The last (fourth) version of mockups as well as the preference editor, which will be presented in chapters 6 and 7, have especially been designed with the objective to meet those requirements.

Part of the work reported in this deliverable is still work in progress. The last user interface iteration and the policy editor still need to be tested and their implementations need to be completed. Also, more work in the area of policy icons is planned. Results of this future work will be reported in the final HCI Research Report D4.1.5, which will be due at the end of project year three.

1.3 Methodology

For the development of policy display and management mockups, we have followed an iterative design based on a cyclic process of UI (User interface) prototyping, usability testing (of the first two iterations), and subsequent refinements and redesigns of the user interfaces.

The second and third mockup iterations have been tested with guided usability tests, followed by post-test interviews with 5 test persons each. Nielsen [28] points out that while experiments showed that a test with at least 15 users is needed to discover all the usability problems in the design, it is better to distribute the budget for user testing across several iterations of mockup developments/improvements and tests, e.g. it will be better to spend this budget on three tests with 5 users each. After the first study with 5 users, usually 85% of the usability problems will be found, and it is recommended to fix these problems in a redesign before testing again. For this reason, we have also decided to do a series of iterations of mockups redesigns for our policy mockups and tested the early iterations with only 5 test persons in each iteration round. The fourth mockup iteration will however be tested with a larger number of test users.

The reader should also note that in iteration, larger redesigns were done. This is not uncommon if user interfaces for new applications (such as for PPL and for “on the fly” policy management) are designed. The reason for this is that each test revealed relevant usability issues that had to be addressed by the next iterations. Besides, some HCI requirements derived from PPL were only specified at the time when we designed the fourth mockup iteration.

Still all three mockup iterations presented in the deliverable, have some core aspects in common. In particular, all use the approach of displaying policies in multiple layers (as suggested in [3]) and all iterations are summarising policy information about what data is requested for what purposes on the top layers with the help of two-dimensional tables. Besides, all mockups allow the users from a set of predefined privacy preferences which can be configured “on the fly”.

1.4 Related work

The Article 29 Data Protection Working Party has investigated what information should be provided in what form to users in order to fulfil all legal provisions of the EU Data Protection Directive 95/46/EC for ensuring that individuals are informed of their rights to data protection [3]. The Art. 29 Working Party recommends providing information in a “multi-layered format under which each layer should offer individuals the information needed to understand their position and make decisions”. They suggest three layers of information provided to individuals: The short notice (layer 1) must offer individuals the core information required under Art. 10 DPD, which includes at least the identity of the controller and the purpose of processing. In addition, a clear indication must be given as to how the individual can access additional information. The condensed notice (layer 2) includes in addition all other relevant information required by Art. 10 DPD of the Directive such as the recipients, whether replies to questions by the data controller are obligatory or voluntary and information about the data subject’s rights. The full notice (layer 3) includes in addition to layers 1 and 2 also “national legal requirements and specificities.”

Recent work on a “Nutrition Label” for privacy [4], has been proposing how to present information to be displayed in short privacy notices, namely the types of information to be collected, how this information is used and with whom it may be shared, in a user-friendly manner. In particular, a visualisation technique for displaying policies in a two-dimensional grid with “types of information” that are requested as rows and purposes as columns was developed and well perceived by test users. Our policy display mockup iterations, which will be presented in chapters 4, 5, and 6, we have also used and tested two-dimensional table presentations, which are similar to the proposed grid, for summarising what data is released to whom for what purposes.

Our UI prototypes for policy display are based on the Art. 29 Working Party Recommendation. In addition, we investigate how this approach of multiple layers can be extended by adding standardised icons for privacy policies or policy elements to the short notices at the top layer. Our work and further related work on privacy policy icons, such as the policy icon proposals by [5] and [6], are reported in chapter 3 of this deliverable.

Further previous work on privacy policy related HCI aspects comprises work on facilitating privacy policy authoring and management in organisations [7], [8]. The SPARCLE Policy Management Workbench allows users to construct services sides' policies using a natural language interface [9]. The emphasis of the HCI (Human Computer Interaction) work in WP4.3 has however been on the display and management of policies at the user side. More HCI work on policy administration at the services side is however planned within PrimeLife for the last project year.

Moreover, there has been also previous work on the usability of P3P³ user agents [10], and means for mediating information of P3P privacy policy compliance by websites to end users [11], [12], and on user interface designs for allowing end users to influence policies by dictating obligations [13]. The related work on usability of P3P for end users is, however, not taking compliance with EU privacy legislation into consideration.

The Privacy Bird⁴ is a P3P user agent that allows the user to specify her privacy preferences regarding a website's data handling policy. The privacy bird uses the traffic light metaphor for displaying information about the compliance of a site's policy with the user's preferences: If a site's policy meets the user's preferences, a small green bird icon in the browser's title bar emits a happy tweet after the page has been loaded. If the site violates the user's privacy preferences, the bird icon turns red and chirps a shrill warning when the page is first loaded. For sites that are not having a P3P policy, a yellow bird will appear. It is however questionable whether the traffic light is the right metaphor in this context, because having no privacy policy (symbolised by the yellow bird) can actually be regarded as worse than having a policy not matching the user's preferences (symbolised by the red bird). For allowing users to specify their privacy preferences, a set of three predefined preference settings is provided, which can be customised by the user during the installation process and via the privacy-bird menu. However, in contrast to the approach that we have taken, the privacy bird does not permit to define more fine-grained privacy preferences, which could for instance be conditioned on individual data controllers and data values. Moreover, the privacy bird also does not allow changing privacy preference settings semi-automatically "on the fly".

In contrast to the PrimeLife Policy Language (PPL), for which the last iteration of our user interfaces were specifically designed, P3P has several functional restrictions, in particular it lacks support for obligations, support for downstream data sharing as well as support for anonymous credentials. Besides, P3P has only a focus on one type of interactions (web pages, http).

1.5 Main Contributions

In comparison to previous work, this deliverable provides in particular the following main contributions:

- We contribute with a comprehensive set of policy icons which are enhancing the ones suggested previously by [5] and [6] and which are in particular meeting requirements derived from European privacy legislation. We also report about the results of the first intercultural user tests for policy icons that has been conducted by us;

³ Platform for Privacy Preference project, <http://www.w3.org/P3P/>

⁴ <http://www.privacybird.org/>

- First ideas and concepts for icons for email usage are reported;
- We contribute with a series of novel user interfaces for allowing end users to manage their privacy preferences “on the fly”;
- We present the first user interfaces for privacy policy display and management that are specifically designed to meet technical requirements of the PrimeLife Policy Language (PPL).

1.6 Terms and definitions

In the remainder of this deliverable, we use the terms “privacy preferences”, “release policy” and “privacy settings” interchangeably. “Privacy preferences” is the traditional term, which is used in P3P and also in the PrimeLife Policy language PPL to express under which conditions the uses would like to release what kind of data. Strictly speaking, “preferences” is however not the best term for conditions chosen or set by the user, which are not optional but that should be binding and can only be explicitly overruled by the user herself. To express that these conditions are not only a preference but requirements set by the users, we have started to use the term “privacy settings” instead of “privacy preferences” in later user interface versions.

Instead of “privacy preferences”, sometimes the short form “PrivPref” has been used.

The Data Protection Directive 95/46/EC defines different roles to which rights and obligations are assigned, and which are therefore also used in the context of privacy policies. These definitions of roles are the following:

A *data controller* is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purpose and means of the processing of personal data.

A *processor* is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

A *data subject* is an identified or identifiable natural person and personal data is any information relating to this identified or identifiable natural person.

A *third party* is any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

1.7 Structure of this Deliverable

The remainder of this deliverable is structured as follows:

Chapter 2 (“Background”) provides a brief overview to the PrimeLife Policy Language PPL developed by PrimeLife Activity 5 and discusses PPL specific requirements for the policy user interfaces developed by PrimeLife Activity 4.

Chapter 3 (“Policy Icons and Tests”) presents a second version of icons for expressing relevant aspects from privacy policies, which are based on the icon set that we have presented in D4.3.1, but which have since the publication of D4.3.1 been further elaborated within task 4.3.2. First test results for these icons are presented as well. Besides, it reports about work in progress and first on icons for e-mail usage and about first results of this work.

Chapter 4 (“Multiple Steps Policy Management and Display Mockups - 2nd Iteration Cycle”) presents the second iteration of UI prototypes for privacy policy display and preference

management, which consists of multiple steps. Usability test results and conclusions drawn from them are presented as well.

Chapter 5 (“Policy Management & Display Mockups –3rd Iteration cycle”) presents the third iteration of UI prototypes for privacy policy display and preference management, which we have developed and tested within PrimeLife. These user interfaces of a so-called “PrimeLife Checkout” have been developed for Online shopping applications. Again, test results and conclusions drawn from them are presented as well.

Chapter 6 (“Policy Management & Display Mockups – 4th Iteration cycle”) presents the fourth iteration of user interface mockups, which was specifically designed to meet the PPL specific HCI requirements.

Chapter 7 (“Privacy Preferences Editor”) describes and illustrates the design of the first version of the privacy preferences editor that we are developing in PrimeLife WP 4.3.

Finally, Chapter 8 (“Conclusions”) draws overall conclusions and provides an outlook to WP 4.3’s future work.

Chapter 2

Background

In this chapter we give a brief overview of the features of the PrimeLife Policy Language (PPL) developed within Activity 5 of this project, and we discuss the requirements for the user interfaces that will be developed by Activity 4 to interact with the PPL engine.

2.1 The PrimeLife Policy Language

The PrimeLife Policy Language (PPL) is an extension of the eXtensible Access Control Markup Language (XACML) [14], the *de facto* standard language for attribute-based access control. Two main extensions that we made to XACML are that we enhance XACML rules so that they can contain *credential-based* access restrictions, and that we add the possibility to, on the data controller's side, specify data handling policies to attributes that the data subject is to reveal, and, on the data subject's side, to attach data handling preferences to pieces of personal information.

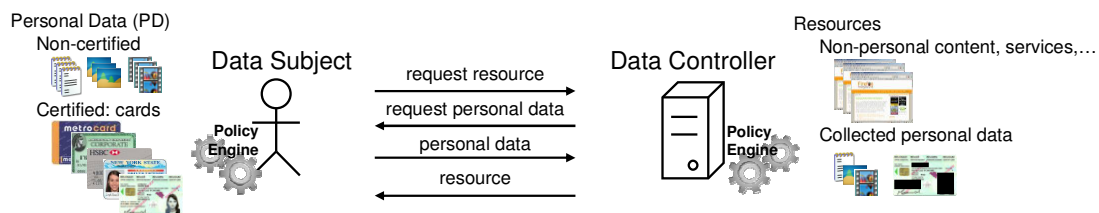


Figure 1. Structure of PrimeLife Policy Language (PPL).

The usage structure of PPL is depicted in Figure 1. Structure of PrimeLife Policy Language (PPL). On the data controller's side, a PPL engine protects access to the hosted resources, which could include web pages and services, as well as previously collected personal data that is forwarded to downstream data controllers. On the data subject's side, a PPL engine protects access to the data subject's personal information, which may include attributes of certified credentials (or cards), as well as other non-certified information (e.g., email addresses or pictures).

In a typical interaction, the data subject first requests access to a resource that she is interested in. The data controller responds with the applicable access control policy for the resource, which includes the credentials that the user has to own, the (certified or non-certified) attributes that she

has to reveal, and the data handling policies. The data subject will check whether she is able to satisfy the access control policy, and whether her preferences match the proposed data handling policies. Interaction with the user may be required to select a combination of personal information to reveal in case there are multiple ways for her to satisfy the access control policy (so-called identity selection), and to obtain the user's permission to overrule her own preferences in case of a mismatch between the proposed policy and her preferences. If either a match is obtained, or all mismatches are overruled, a sticky policy is created that describes the exact terms under which the data is released. Once a matching set of personal information is decided upon, the personal data and the associated sticky policies are sent to the data controller. The data controller performs a number of checks to make sure that the transmitted data indeed satisfies his access control policy etc., and sends back the requested resource.

2.1.1 Basics of XACML

XACML defines an XML-based language as well as a processing model for evaluating the policies on the basis of a given XACML access request. Such request specifies by means of attributes which subject (i.e., who) wants to perform which action (i.e., do what) on which resource (i.e., on what).

An XACML policy has a PolicySet root element that further contains Policy or PolicySet elements. A Policy contains a set of Rules that define positive or negative authorizations (Permit or Deny rules). The Rule, Policy and PolicySet elements may contain a Target that determines their applicability, i.e., to which access requests the respective elements and their children apply. The Target is expressed in terms of simple combinations of attributes describing applicable subjects, actions and resources. The applicability of a Rule is further determined by a boolean Condition that allows for more complex restrictions by means of functions over such attributes. Functions are stated by means of Apply elements that specify a respective FunctionID XML-attribute (e.g., 'string-equal') and that contain child elements representing the appropriate function parameters. Such parameters may be: (1) AttributeDesignator elements referring to attributes given in the request, (2) concrete attribute values, or (3) further Apply elements. Each PolicySet and Policy element also specifies a combining algorithm defining how to combine the different outcomes of the contained child elements (i.e., Policy, PolicySet, and Rule elements, respectively) when a request is evaluated with respect to an XACML policy.

2.1.2 Credential-based extensions in PPL

In credential-based access control [15], [16], [17], [18], also called *card-based* access control, attributes are bundled together in credentials (or cards) owned by the data subject. The issuer of a credential vouches for the correctness of the attribute values with respect to the credential owner. Not only does this abstract view on credentials intuitively mirror the real-world authentication cards found in every citizen's wallet today, it also acts as an excellent model to unify authentication technologies as diverse as SAML, OpenID, X.509 certificates, trusted LDAP servers, WS-Trust, and most importantly for this project because of the privacy advantages that they offer, anonymous credentials [19], [20], [21]. The latter technology enable the data subject to selectively reveal subsets of attributes from a credential, and even to merely prove that the attributes contained in a credential satisfy a certain condition, without revealing the exact attribute values. All of this is performed while preserving untraceability and unlinkability between different uses of the same credential.

The language extensions that PPL introduces to XACML go beyond the standard extension points of XACML. All proposed extensions are in line with the semantics of existing XACML language constructs though, i.e., it does not alter the semantics of existing elements or attributes. Since it

does not make sense to require a user to *not* own certain credentials (the user can always pretend not to own them [18] below), XACML rules that contain credential requirements can only have effect Permit. Rules with effect Deny are pointless as they essentially require the requester *not* to show a certain credential. Assuming that the requester's goal is to obtain access, she can always pretend not to have the specified credentials.

Our extensions enable policy authors to express conditions on the credentials that a requester must own and the actions that she must perform to be granted access. To this end PPL augments the Rule element with optional CredentialRequirements and ProvisionalActions child elements. The former describes the credentials that the requester needs to own and the conditions that these credentials have to satisfy. The latter describes the actions that she has to perform. We now discuss both elements in more detail.

To express credential-based access control policies, the language needs a way to refer to the credentials that bundle several attributes together. For example, it must be possible to refer to the requester's name as it appears on her passport, not on her credit card. Cross-credential conditions are another important use case: for example, the policy language must allow one to express that the names on a credit card and on a passport must match, or that the expiration date of an entry visa is before the expiration date of a passport.

To this end, CredentialRequirements contains a Credential child element for each credential involved in the rule, which is assigned a (rule-wide unique) identifier CredentialId as an attribute. The Credential can contain AttributeMatchAnyOf child elements to compare an attribute of that credential to a list of values. The CredentialRequirements also contain a Condition where conditions on the credentials' attributes can be expressed. Inside a condition, one can refer to an attribute AttributeId within a particular credential by means of CredentialAttributeDesignator which takes both CredentialId and AttributeId as attributes.

Conditions on credential attributes are expressed using the same schema as the XACML Condition element, extended by the CredentialAttributeDesignator element mentioned above. Conditions can contain any combination of restrictions on any credential attributes, including the issuer and the type of the credential. For matching credential types, PPL introduces a new function subtype-of that checks whether the presented credential is of a subtype of a specified credential type as per the credential type ontology.

The ProvisionalActions element contains the actions that have to be performed by a requester prior to being granted access. The types of actions that we model are:

- **Consent:** The requester has to explicitly consent to a given statement, e.g., the terms of service. How consent is given could depend on the underlying technology: it could for example involve a cryptographic signature, or simply a click on a button in the user interface.
- **Attribute disclosure:** Rather than assuming that all attributes of a credential are revealed by default, the policy explicitly lists which attributes of which credential need to be revealed. Moreover, in order to fully leverage the power of privacy-enhancing technologies such as anonymous credentials that allow the requester to prove conditions without revealing the attribute values, this list does *not* (necessarily) include the attributes that occur in the conditions. Apart from the attribute and credential identifiers, the requirement to reveal an attribute can optionally refer to the data handling policy that describes how the attribute value will be treated after it is received. Data handling policies are discussed in the next subsection. Also, the action can optionally specify to whom the attribute value is to be revealed, in case this is not the data controller himself but some third party. This can be used for example to specify that the user's address has to be given to the shipping company, but that the data controller himself has no use for it.

- **Consumption control:** Consumption control allows the policy author to impose limitations on how often the same credential can be used to obtain access. For example, one could impose that each ID card can only be used once to vote in an online opinion poll. A consumption control statement has to specify the credential to be consumed, the number of units to spend, the limit of units that can be spent in total, and a “consumption scope”. We refer to [17] for details on their exact semantics.

PPL leaves open the possibility to add new types of provisional actions later by a mechanism similar to the one used for defining functions in XACML. Namely, each provisional action is contained in a `ProvisionalAction` element that includes an action identifier as an attribute `ActionId`. We define action identifiers for the action types above, but allow users to add more identifiers later.

2.1.3 Data handling extensions in PPL

PPL also defines extensions to XACML rules to allow data controllers (i.e., servers) to specify the data handling policies describing how requested attributes will be treated, and to allow data subjects (i.e., users) to specify preferences describing how they expect their personal information to be treated.

Data handling policies are contained in `DataHandlingPolicy` elements and have a unique identifier `PolicyId` by which they can be referred to from a `RevealUnderDHP` provisional action statement, i.e., a provisional action requiring to reveal an attribute under a particular data handling policy. On the data subject’s side, data handling preferences are contained in `DataHandlingPreferences` elements. The attributes or personal information to which they apply are specified by means of the `Target` of the rule, as is done in standard XACML.

Both data handling policies and preferences are composed of a set of authorizations and a set of obligations. Data handling policies describe the authorizations that the data controller *wants* to obtain with respect to the data, and the obligations he *is willing to promise* to adhere to after receiving the data. Data handling preferences specify the authorizations that the data subject *is willing* to give away for the data, and the obligations that she *requires* to be adhered to.

The lists of supported authorization and obligation types are extensible, but PPL supports a number of built-in types “out of the box”. For authorizations, two types are defined:

- **Use for purpose:** When part of a data handling policy, this authorization states the list of purposes for which the data *could* be used; when part of the preferences, it states the list of purposes for which the data *can* be used. The list of supported purposes is again user-extensible, but a basic list based on P3P is supported “out of the box”.
- **Downstream usage:** When part of a data handling policy, this authorization simply expresses that the data controller intends to forward the data to downstream data controllers, but is willing to impose any restrictions that the data subject requires. When part of the preferences, this authorization specifies that the data can be used downstream, and optionally specifies a PPL policy that the data controller has to impose on any downstream data controllers.

Obligations are structured as “on *trigger* do *action*” statements. The list of supported triggers and actions is again user-extensible, but PPL has the following types built in:

- **Trigger at time:** A one-time event that triggers at a particular time.
- **Trigger periodic:** A repeated event that occurs at regular time intervals.
- **Trigger accessed for purpose:** The event that the personal information is accessed for a particular purpose.

- **Trigger deleted:** The event that the personal information is deleted.
- **Trigger sent:** The event that the personal information is forwarded to a downstream data controller.
- **Trigger accessed by data subject:** The event that the personal information is being accessed by the data subject herself.
- **Trigger data lost:** The event that the personal information has been lost through a data leakage or breach.
- **Trigger on violation:** The event that the agreed-upon sticky policy has not been adhered to.
- **Action delete:** The action to delete the data.
- **Action anonymize:** The action to anonymize the data.
- **Action notify data subject:** The action to notify the data subject.
- **Action log:** The action to write an entry to a log.
- **Action secure log:** The action to write an entry to a secure log.
- **Action give access:** The action to let a specific party access the data.

We refer to the PPL draft specification [22] and the work by Bussard, Neven, and Preiss [23] for details on the matching of data handling preferences against policies.

2.1.4 Example policy

The following is a sample PPL policy describing the access control restrictions to subscribe to an online shop www.store.com. In summary, the rule depicted below expresses the following:

- Data handling policy #DHP1:
 - use for purpose statistics, administration, marketing
 - share downstream
 - delete after one year
- Data handling policy #DHP2:
 - use for purpose: payment
 - no sharing downstream
 - delete after one month
- Own eID card from Belgian government and Visa or American express credit card so that
 - older than 18 by birth date on eID
 - credit card has not expired
 - name on eID card matches that on credit card
- Reveal (uncertified) email address under #DHP1
- Reveal address from eID card under #DHP1
- Reveal credit card number and expiration date under #DHP2

```
<ppl:Policy xmlns:cr="http://www.primelife.eu/ppl/credential"
  xmlns:ob="http://www.primelife.eu/ppl/obligation"
  xmlns:ppl="http://www.primelife.eu/ppl"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyId="policy1" RuleCombiningAlgId="PermitOverrides">

  <xacml:Target>
    <xacml:Resources>
      <xacml:Resource>
```

```

<xacml:ResourceMatch
  MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
  <xacml:AttributeValue DataType="xs:anyURI">
    http://www.store.com/subscribe.html
  </xacml:AttributeValue>
  <xacml:ResourceAttributeDesignator DataType="xs:anyURI"
    AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
  </xacml:ResourceMatch>
</xacml:Resource>
</xacml:Resources>
</xacml:Target>

<ppl:DataHandlingPolicy PolicyId="#DHP1">
  <ppl:AuthorizationsSet>
    <ppl:AuthzUseForPurpose>
      <ppl:Purpose>
        http://www.w3.org/2006/01/P3Pv11/statistics
      </ppl:Purpose>
      <ppl:Purpose>http://www.w3.org/2002/01/P3Pv1/admin</ppl:Purpose>
      <ppl:Purpose>http://www.w3.org/2006/01/P3Pv11/marketing</ppl:Purpose>
    </ppl:AuthzUseForPurpose>
    <ppl:AuthzDownstreamUsage allowed="true" />
  </ppl:AuthorizationsSet>
  <ob:ObligationsSet>
    <ob:Obligation>
      <ob:TriggersSet>
        <ob:TriggerAtTime>
          <ob:Start>
            <ob:StartNow/>
          </ob:Start>
          <ob:MaxDelay>
            <ob:Duration>P1Y</ob:Duration>
          </ob:MaxDelay>
        </ob:TriggerAtTime>
      </ob:TriggersSet>
      <ob>ActionDeletePersonalData/>
    </ob:Obligation>
  </ob:ObligationsSet>
</ppl:DataHandlingPolicy>

<ppl:DataHandlingPolicy PolicyId="#DHP2">
  <ppl:AuthorizationsSet>
    <ppl:AuthzUseForPurpose>
      <ppl:Purpose>http://www.w3.org/2006/01/P3Pv11/payment</ppl:Purpose>
    </ppl:AuthzUseForPurpose>
    <ppl:AuthzDownstreamUsage allowed="false" />
  </ppl:AuthorizationsSet>
  <ob:ObligationsSet>
    <ob:Obligation>
      <ob:TriggersSet>
        <ob:TriggerAtTime>
          <ob:Start>
            <ob:StartNow/>
          </ob:Start>
          <ob:MaxDelay>
            <ob:Duration>P1M</ob:Duration>
          </ob:MaxDelay>
        </ob:TriggerAtTime>
      </ob:TriggersSet>
      <ob>ActionDeletePersonalData/>
    </ob:Obligation>
  </ob:ObligationsSet>
</ppl:DataHandlingPolicy>

<cr:CredentialRequirements>
  <cr:Credential CredentialId="#eid">
    <cr:AttributeMatchAnyOf AttributeId="cr:Issuer">
      <cr:MatchValue DataType="xs:anyURI">

```

```

    MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
      http://www.fgov.be
    </cr:MatchValue>
  </cr:AttributeMatchAnyOf>
<cr:AttributeMatchAnyOf AttributeId="cr:CredentialType">
  <cr:MatchValue DataType="xs:anyURI"
    MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
    http://www.fgov.be/eID
  </cr:MatchValue>
</cr:AttributeMatchAnyOf>
</cr:Credential>

<cr:Credential CredentialId="#creditcard">
  <cr:AttributeMatchAnyOf AttributeId="cr:Issuer">
    <cr:MatchValue DataType="xs:anyURI"
      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
      http://www.visa.com
    </cr:MatchValue>
    <cr:MatchValue DataType="xs:anyURI"
      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
      http://www.amex.com
    </cr:MatchValue>
  </cr:AttributeMatchAnyOf>
  <cr:AttributeMatchAnyOf AttributeId="cr:CredentialType">
    <cr:MatchValue DataType="xs:anyURI" MatchId="cr:subtype-of">
      http://www.banking.org/CreditCard
    </cr:MatchValue>
  </cr:AttributeMatchAnyOf>
</cr:Credential>

<cr:Condition>
  <xacml:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
    <cr:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
      less-than-or-equal" Disclose="attributes-only">
      <cr:CredentialAttributeDesignator CredentialId="#eid"
        DataType="xs:date" AttributeId="http://www.fgov.be/eID/birthdate"/>
      <xacml:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:
        date-subtract-yearMonthDuration">
        <xacml:EnvironmentAttributeDesignator DataType="xs:date"
          AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-
            date"/>
        <xacml:AttributeValue DataType="http://www.w3.org/TR/2002/WD-
          xquery-operators-20020816#yearMonthDuration">
          P18Y
        </xacml:AttributeValue>
      </xacml:Apply>
    </cr:Apply>
    <xacml:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-
      greater-than">
      <cr:CredentialAttributeDesignator CredentialId="#creditcard"
        DataType="xs:date" AttributeId="http://www.banking.org/CreditCard/
          expirationdate"/>
      <xacml:EnvironmentAttributeDesignator DataType="xs:date"
        AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-
          date"/>
    </xacml:Apply>
    <xacml:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:
      string-equal">
      <cr:CredentialAttributeDesignator CredentialId="#eid"
        DataType="xs:string" AttributeId="http://www.fgov.be/eID/
          firstname"/>
      <cr:CredentialAttributeDesignator CredentialId="#creditcard"
        DataType="xs:string" AttributeId="http://www.banking.org/
          CreditCard/name"/>
    </xacml:Apply>
    <xacml:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:
      string-equal">
      <cr:CredentialAttributeDesignator CredentialId="#eid"

```



```

        DataType="xs:string" AttributeId="http://www.fgov.be/eId/
        lastname"/>
    <cr:CredentialAttributeDesignator CredentialId="#creditcard"
        DataType="xs:string" AttributeId="http://www.banking.org/
        CreditCard/surname"/>
    </xacml:Apply>
</xacml:Apply>
</cr:Condition>
</cr:CredentialRequirements>

<ppl:ProvisionalActions>
    <ppl:ProvisionalAction
        ActionId="http://www.primelife.eu/ppl/RevealUnderDHP">
        <xacml:AttributeValue DataType="xs:anyURI">
            http://www.w3.org/2006/vcard/ns#email
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            #DHP1
        </xacml:AttributeValue>
    </ppl:ProvisionalAction>
    <ppl:ProvisionalAction ActionId="http://www.primelife.eu/ppl/
        RevealUnderDHP">
        <xacml:AttributeValue DataType="xs:anyURI">
            http://www.fgov.be/eID/address
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            #DHP1
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">#eid</xacml:AttributeValue>
    </ppl:ProvisionalAction>
    <ppl:ProvisionalAction
        ActionId="http://www.primelife.eu/ppl/RevealToUnderDHP">
        <xacml:AttributeValue DataType="xs:anyURI">
            http://www.banking.org/CreditCard/cardnumber
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            http://www.ogone.com
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">#DHP2</xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            #creditcard
        </xacml:AttributeValue>
    </ppl:ProvisionalAction>
    <ppl:ProvisionalAction
        ActionId="http://www.primelife.eu/ppl/RevealToUnderDHP">
        <xacml:AttributeValue DataType="xs:anyURI">
            http://www.banking.org/CreditCard/expirationdate
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            http://www.ogone.com
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            #DHP2
        </xacml:AttributeValue>
        <xacml:AttributeValue DataType="xs:anyURI">
            #creditcard
        </xacml:AttributeValue>
    </ppl:ProvisionalAction>
</ppl:ProvisionalActions>

</ppl:Policy>

```

2.2 User interface requirements

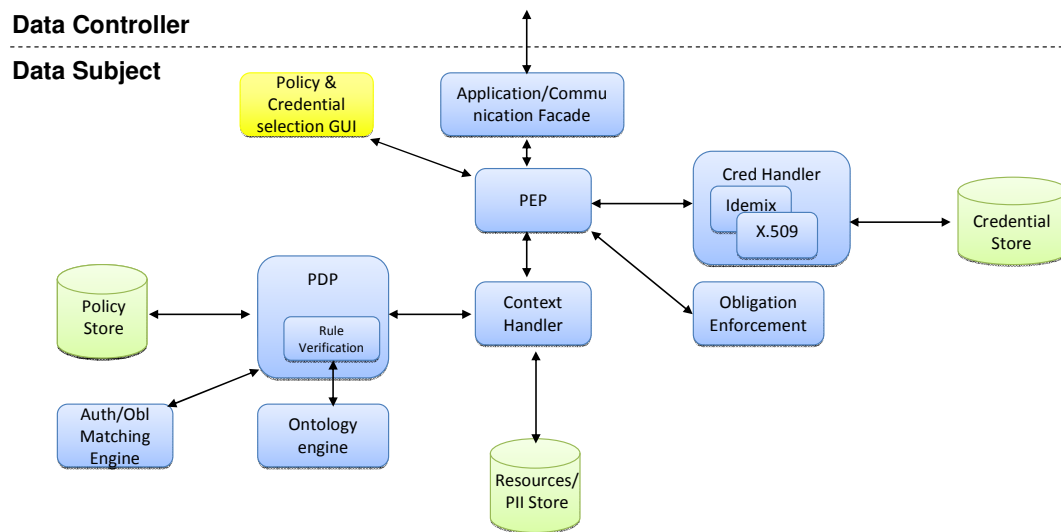


Figure 2. PPL engine architecture

There are several points in the deployment of a PPL engine where interaction with the user is required, both on the data subject's and on the data controller's side. Figure 2. PPL engine architecture depicts the architecture of the PPL engine on the data subject's side. (Since both the data subject and the data controller run a PPL engine to protect their resources, a similar architecture is present on the data controller's side.) The component "policy & credential selection GUI" is called to consult the user on which credentials to use to authenticate, to display the (possibly mismatching) sticky policies, and, in case a mismatch occurs, to prompt whether the mismatch should be overruled. Two other user interface components, the policy and preference editors, are not displayed in this picture, as they are not part of the core engine architecture. We give more details on the particular requirements for the different interfaces below.

2.2.1 Credential selection

After receiving the applicable PPL policy for the requested resource, the PPL engine on the data subject's side will check the list of owned credentials (stored in the credential store) and the list of uncertified PII (stored in the PII store) to see which combinations of credentials and PII can be used to satisfy the policy. When multiple combinations are possible, the credential selection GUI must be invoked to let the user choose which combination should be used for this transaction. The GUI should reflect, in an appropriate level of detail, the exact information that will be revealed when a particular combination is chosen.

Technically it would be easiest to first let the user choose her combination of credentials to use, and only then let the user inspect the resulting sticky policies. From the user's perspective, however, it may make sense to integrate the credential selection and the (mis)matching policy interfaces of Sections 2.2.2 and 2.2.3 below into a single interface to browse through the various combinations of credentials and/or PII and the resulting sticky policies. This would allow the user to base her choice of credentials and/or PII on the (mis)matches with respect to her preferences, which may be desirable in practice.

2.2.2 Matching policy dialog

Even if a match is found between the data subject's preferences and the proposed data handling policies for the chosen combination of credentials and PII, there is a legal requirement that the user gives her explicit informed consent to the data transfer. This means that the user needs to be informed about the details of the transmitted information and the applicable sticky policies. The user interface needs to make a trade-off between simplicity and expressivity: the average user should not be overwhelmed by an abundance of details, but a more privacy-aware user wants to be able to find all the details that she may be interested in.

2.2.3 Mismatching policy dialog

When a certain combination of credentials and/or PII satisfies the access control restrictions, but the proposed data handling policies do not match the data subject's preferences, then in theory we have a mismatch and the transaction should be canceled. In practice, however, this may lead to too many transactions being canceled because of mismatching preferences, possibly causing users to set their preferences to a minimum or switching off the PPL engine altogether. Alternatively, the details of the policy mismatch could be made clear in an interface to the user, who can then make an informed decision on whether to overrule her own preferences or not. She could even choose to remember her choice to overrule, so that less stringent preferences will be used next time when interacting with the same resource or data controller.

2.2.4 Preferences editor

Given their low technical skills, data subjects are obviously unlikely to express their own preferences directly in the XML-based PPL syntax. One solution could be for trusted third parties (e.g., data protection agencies) to compose sample preferences that they deem to be offering an appropriate level of privacy. But for better control of their preferences, users should be offered a user-friendly interface by which they can fine-tune their preferences. Again, a trade-off between simplicity and expressivity will have to be made here. Also, one will have to evaluate whether it is best to develop an interface by means of which the user can set its global preferences, or to use a "self-learning" interface, where at each transaction the user is offered the choice to "remember" her settings. The latter approach is commonly used in personal firewall software today, probably because users are unlikely to invoke a separate application and spend an hour or more to set their security policies once and for all. A similar argument can probably be made for the case of data handling preferences.

Given the similarity of PPL preferences, policies, and sticky policies, it is quite likely that similar user interface elements can be reused across the different editors and dialogs.

2.2.5 Policy editor

Even though the policy author on the data controller's side is more likely to be technically skilled than the data subject, some user interfaces support to design PPL policies could be a great help to set policies correctly. Especially in applications where the policy author is a common user (e.g., a social network user defining the rules who can access her profile information), a highly simplified interface is essential. For example, the interface could use icons that can be automatically translated into (a subset of) the PPL language.

Chapter 3

Policy Icons and Tests

3.1 Introduction

The idea of displaying content of privacy policies with icons has been further developed since the PrimeLife D4.3.1 deliverable. This chapter does not only outline aspects of improving the transparency of data processing for the user by supporting the display of a privacy policy through especially tailored icons. It also describes the motivation for such an approach, as well as limitations, addresses approaches by others in this domain, and gives an overview of elements that need to be expressed through such a system of icons as well as the first attempt of implementing such a set. It furthermore shows first test results our icon development and gives an outlook on the ongoing work with icons. In the outlook, we will also discuss, for which other purposes icons can be used besides of displaying privacy policies components. One approach of using icons is the displaying of special kind of personal data in conjunction with the usage of Social Networking Sites (SNS). In this context, icons could not only display parts of the privacy policy, they could also be used to display privacy aspects according to each transaction that the user will do in the SNS.

3.2 Related work

The idea of expressing relevant statements from privacy policies in abbreviated form using icons was to our knowledge initially published by Mary Rundle [5] (2006). Her idea was to introduce Creative Commons-like icons for the protection of private information. Her approach offers a set of different icons for different purposes and different data types and is based on the U.S. law and U.S. understandings of privacy. The differences between European and U.S. understandings, Rundle's work and its basis on Creative Commons have already been presented in PrimeLife deliverable D4.3.1. As Rundle's approach did not address policy requirements derived from European data protection legislation and did not contain icons as probably necessary to express central purposes and data types which are relevant content of privacy policies, her approach was broadened. The motivation for further development and the legal requirements of European data protection rules in contradiction to U.S. rules have also been discussed in PrimeLife deliverable D4.3.1 [24].

Part of her work is displayed in the table below:








	You agree not to use this data for marketing purposes.
	You agree not to trade or sell this data.
	You agree to submit to a third-party audit program on data use; if government has requested access to my data, you agree to involve my governmental ombudsman.
	You agree to make available to me the data that you have on me without my having to pay for it/at a minimal charge.
	You allow me to address inaccuracies in the data and request its removal.
	You agree to take reasonable steps to keep my data secure.
	You agree to arrange with X organization to help resolve any disputes we have over your treatment of this data. [The seal / name of the entity follows.]

Table 1. Mary Rundle's icon set

Also Martin Mehlau worked on icon sets [6] (2007) and developed a bigger icon set containing icons for more purposes and data types. His work has also been presented in PrimeLife deliverable D4.3.1 [24].

In the table below, an overview of his icon sets is given:

Iconset for Data-Privacy Declarations v0.1

Let's simply declare what data is how used, stored, given away or deleted.

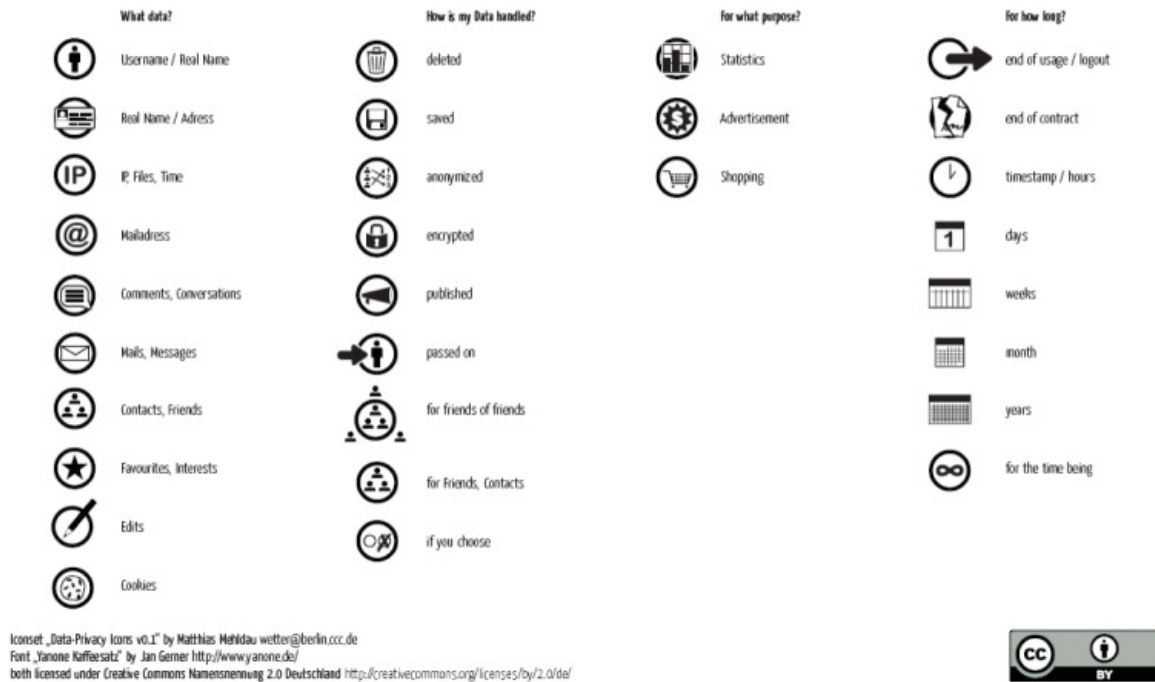


Table 2. Mehldau's approach

Rundle's and Mehldau's work have been the basis for PrimeLife's work on icons. In PrimeLife deliverable D 4.3.1 we presented a first approach of possible icon sets for different categories: icons representing data processing steps, icons representing data types, icons representing groups of recipients and icons representing purposes.

In addition, icons could in principle express core aspects of privacy policies, such as retention periods, steps and purposes of data processing, and possible recipients. PrimeLife has therefore chosen a wide approach, developing a variety of privacy-related icons. This set includes data types, purposes and other information and was called icon set for “general use”. It was, however, in its actual variety only created for usability testing and to provide a basis set for further refinement. Such refinement may be done by creating subsets for specific purposes. For this we have developed an icon set for SNS displaying different aspects which are not automatically content of the SNS privacy policy - but should be from a privacy and transparency point of view. In future steps this system may be extended to certain further use cases, for example to show limitations that the sender of an e-mail or other messages wants the recipient to be aware of (e.g., retention period, right to further disseminate the messages content). Using e-mails typically is not combined with privacy policies. Nevertheless it also includes various aspects of using personal data which the user is not automatically aware of. This can be supported by using e-mail icons. Such a set for use with e-mail is currently developed by researchers at the Stanford University in cooperation with PrimeLife personnel and interested individuals. This approach will be presented in section 3.7.

3.3 Advancement of icon approaches in year 2

In prosecution of PrimeLife deliverable D4.3.1 the motivation for and limitations of icons will be displayed shortly in this chapter with a particular review of the related work and a comparison with the work of year 2.

In general, icons are used to visualize specific statements or properties, e.g. for emergency fire exits or subway stations. Well designed icons allow for quick comprehensibility for everybody who is not visually impaired.⁵ In information and communication technology, icons are widely used, e.g., as visual elements in the user interface for using different functions in applications or as warning or information signs. They are also easy to learn and therefore a good approach to enhance user's privacy awareness. Using icons to express the relevant information on what is going to happen to personal information released by a user could significantly enhance user experience, and might even support transparency, as will be shown.

In the area of privacy policies, some basic icons have been used to show a match or mismatch between the user's preferences and the web service's privacy policy, e.g., in the Privacy Bird.⁶ Moreover, the visual elements for privacy seals can be regarded as icons, which express that the legal compliance of a product or service has been certified. These seals by themselves do not inform the users about specifics of the data processing, but usually they refer with a specific number to an audit report which can be looked up or which is already linked to the graphical representation of the privacy seal.⁷

Legislation on privacy varies largely across jurisdictions. While in EU jurisdictions privacy legislation is harmonised by EU Directives, the European law differs largely from regulations in the US or Asia. Therefore the information relevant for the user may also vary considerably between those regulatory frameworks. For example, while in the US expressing that the data controller accredits the rights to access and rectify personal data might be important information for users such rights are mandatory part of and EC legislation.

Driven by the fact, that privacy policies often are not read, due to their length as well as the lack of comprehensibility and the legal diction, Art. 29 Working Party proposed the concept of layered privacy policies [3]. The working paper, however, does not discuss the use of icons. Layered privacy policies suggest expressing only the most important statements of a privacy policy in the first, most abstract, layer and then giving more details in further layers. Depending on the icons and their relation to data fields they can be very abstract (e.g., making clear that some data are stored) or very specific (e.g., visualizing a specific step of data processing, such as encryption). Clearly the use of icons alone, i.e., without a written privacy policy spelling out the details, cannot be a sufficient substitute for the information that has to be provided to the user. Thus, they can be used in association with a written privacy policy. It is important to note that the documents from the Art. 29 Working Party do not oppose the idea of icons. Catchy icons may be much more attractive and informative for a large group of people than lengthy texts in a technical or legal language.

In the area of privacy, there are until now only very few icons for data processing and none of them standardised. These icons should be clear and understandable even for users, who usually are not aware about privacy aspects and notice the icons for the first time. As icons require the

⁵ To ensure the accessibility also for ability impaired users, icons should be equipped with an explanatory text displayed in accordance with accessibility guidelines such as those published by the Web Accessibility Initiative of the world wide web consortium (see: <http://www.w3.org/WAI/guid-tech.html> last visited 23. June 2009). This would ensure that assistive technologies such as text-to-speech and Braille-bridges will be able to parse the information given. Earcons, brief sound patterns, could also be used to further raise the attention users. Matching of privacy policies and users preferences is also illustrated with sound within privacy bird, online: <http://www.privacybird.org/>.

⁶ See <http://www.privacybird.org/>.

⁷ See for example the European Privacy Seal, EuroPriSe: <https://www.european-privacy-seal.eu/> and the Privacy Seal issued by the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): <https://www.datenschutzzentrum.de/guetesiegel/>.

recipient to get used to their meanings, independent of their expressiveness, a wide acceptance of one set of icons is necessary to ensure recognition by the users.

Note that the meaning of icons is not limited to each specific icon on its own, but the combination of icons may be relevant for the interpretation. This also encompasses the meaning of missing icons: Think of a web service which presents a few icons on its privacy policy, but does not show an icon regarding any possible recipients of the user's data. Here the non-statement concerning a possible data transfer to a recipient could mean that there is no third party receiving the data at all or that a data transfer is not excluded but may happen from time to time, or even that there are regular recipients but the data controller has not put the icon on the website although there may be a statement in the full privacy policy. This example shows the necessity of a detailed description of the "icon language" which may require to put up an icon on existing or non-existing data transfer and possible recipients.

At the same time, legal mechanisms would need to ensure that the meaning the user has learned to be expressed by the icons reflects the practise of the data processors and the data controllers. This can be done by using a trademark protection regime on the icons, where a license to use the trademark is only given to those binding themselves to processing within the expressed meaning. In the domain of governmental certification, also a specific law regulating the uses of certain icons could prove useful.

The domain of privacy statements is too complex to be fully explained by a small set of simple icons because they lack the degree of detail required for a valid informed consent as required by the EU Data Protection Directive 95/46/EC.

As stated above in section 3.1, iconography will not be able to replace full privacy policies nor may icons replace the necessary depth of explanations for the planned use of personal data (purposes) as it is necessary for a valid informed consent (cf. Art. 2 (h) Data Protection Directive 95/46/EC). But icons are able to offer valuable information on a first-glance basis for users and point to core issues related with the processing in a given case. Imagine, e.g., an icon for data to be transferred to another party: The sole information that data are transferred is rather limited. It is also necessary to state, which type of data will be transferred to whom, plus the purpose for the transferral and further processing. Let alone the fact that the retention period and other information are also necessary for users who want to understand what is being done with their data. Therefore the icons should be used in conjunction with links or mouse-over functionalities offering further explanations to the icons and leading the user to the concerning part of the written privacy policy. In addition, the use of icons alone would not increase user's awareness in the proper way. To increase icons functionality it should not only address people with good eyesight; here it is unavoidable to offer alternatives for, e.g., blind people such as alternative texts in HTML-pages or ASCII-representations.

Early and later on within the process of elaborating the icon set, it had been discussed to keep the number of icons low.⁸ It was assumed that icons may be combined, negated (e.g. by crossing out) or defined more precisely with additions (e.g. by adding a duration) and to add an indication for the layer of privacy in relation to the displayed subject could keep the number of necessary icons low. Therefore one aim was still to develop icon sets only for those purposes and data types, users often cope with in the online world.

⁸ During the open space workshop organized by the EC-funded project PrivacyOS in Berlin in April 2009 there had been two sessions on the possible use of icons to resemble privacy related information, in particular the content of privacy policies. Minutes of the sessions are available online: <https://www.privacyos.eu/wiki/index.php/PrivacyRightsAgreements>. The icons have also been topic of discussions during the PrimeLife general meetings in Dresden in October 2009 and Bergamo in March 2010.

3.4 Update on PrimeLife icon set

The previous approaches of icons by Mehldau and Rundle have already been presented in PrimeLife deliverable D4.3.1 [24].

Their shortcomings in displaying special purposes (or in displaying too many different purposes with too many different icons) lead to further research and the development of the PrimeLife icon sets. Thus, some of the purposes or data types included in the PrimeLife icon sets have not been addressed by the first approaches. Another reason for this was the fact that the first approach of Mehldau contained too many different icons and therefore was too complex to understand for the average user. As icons for usage on websites still have to be introduced to a bigger audience, it is important not to overstrain the average user with too many icons to learn. Otherwise the users may not accept the icons.

To focus the attention of the user, it seems helpful to concentrate on icons that point out possible risks, important data transactions and other content that users usually search for in privacy policies or where the law provides specific requirements like for the processing of special categories of data, see. Art. 8 (2) (a) Data Protection Directive 95/46/EC. The selection of potentially dangerous processing steps is done without any prejudice or moral evaluation: While for example hidden profiling of users' behaviour or interests for purposes of targeted advertising will regularly be opposed by users, precise profiling techniques can determine the true value of employee assessment or services that search for possible friends or partners with similar interest profiles. Thus, the icon set attempts to cover those potentially processing steps such as passing on personal data to third parties, profiling or collecting data from different sources to aggregate them, which users often have to deal with without realizing the actual privacy implications of the transaction every time.

As the set of purposes combined with a written policy could be a central element of understanding privacy policies and as it is also important for judging the legitimacy of processing, it was also considered to create icons depicting purposes. However, as there is a high number of purposes, it is hard to depict them in an easily understandable manner. Instead of depicting all purposes some categories of recipients and data types were added to the icon set.

However, to make it more likely that the icons will be adopted, it is necessary to strike a balance and to include symbols that enable data controllers to show their efforts to preserve users' rights to privacy. For this purpose, processing steps which are perceived in a positive way such as encryption or anonymisation of initially personal data are included as well as the possibility to indicate that certain techniques are not deployed by crossing out an icon, thus negating its statement.

As mentioned above, icons representing purposes of data processing were also introduced by Rundle (2006) excluding the sale of data or the use for marketing purposes and by Mehldau (2007) indicating the use of personal data for statistics, advertisement or shopping. However, due to the freedom of contract and the wide variety of thinkable business cases that somehow involve processing of personal data – either as an integral element or as information necessary to perform the contract – it currently does not seem possible to produce a set of icons that is able to accurately represent the variety of purposes. Thus, the written text of the privacy declaration needs to be referred to for explaining the intended use of personal data. However, the icons representing the relevant processing steps may help to point the user's attention to the relevant sections within the written policy.

These icons were also displayed in PrimeLife deliverable D 4.3.1. In the same deliverable the use of icons in direct relation with the privacy policy in form of initials to the individual paragraphs of the policy has been suggested.

3.5 Icon set development during year 2

As mentioned above, the icon sets by Mary Rundle and Martin Mehldau have been the basis for the developed icon sets of PrimeLife. Some of Rundle's and Mehldau's ideas have been combined and adapted with PrimeLife's own approaches to two icon sets: icons for SNS and icons for general use.

In the icon set for general use, data types are defined as well as icons for data handling like collecting, processing and storing. The icon set for SNS includes additional icons for displaying typical aspects of SNS, which would be difficult to display only with the first set. These icons could not only be used to display the SNS privacy policy but also to visualize possible data transactions by the user herself. Thus, the user's privacy awareness in SNS could be strengthened with the icons for SNS.

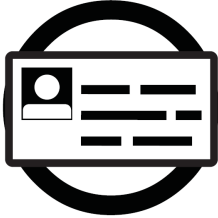


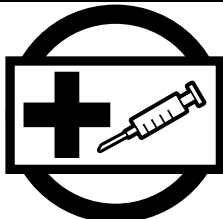

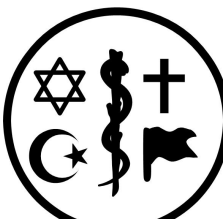
The first icon set approach of PrimeLife had some shortcomings. First of all, it included too many different icons for too many different purposes or data types and was therefore probably a bit too complicated to learn and understand for the average user. Besides of this, some of the icons had shortcomings in their design and therefore were misunderstood. Thus, two new sets were developed on basis of the icons presented in D4.3.1. Some of the icons of the first approach have been kept unchanged; others have been improved or removed.

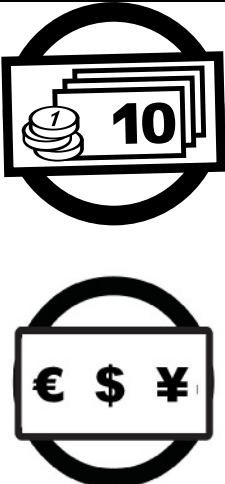
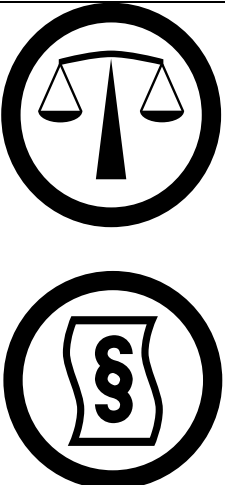
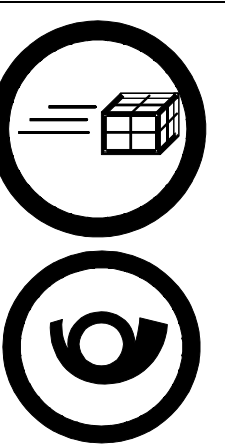
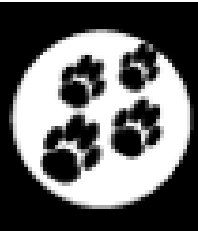
The aim of the further icon development within PrimeLife will still be the reduction of the amount of different icons. The broad set with several redundant entries for the same meaning has been put to first smaller user test with Swedish and Chinese students and is currently put on a larger user test. Once that we will know how the different icons are perceived and whether the concepts to be displayed are understood by the test persons, some further selections will be done. Some icons may disqualify as users do not understand them at all, leaving an alternative with the same meaning or showing the need for further development.



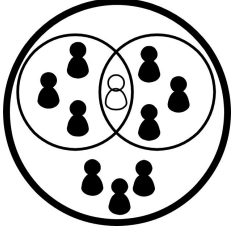
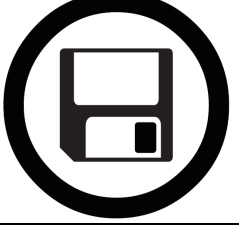

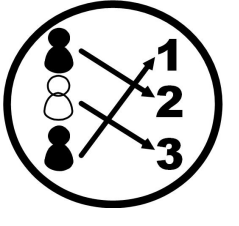
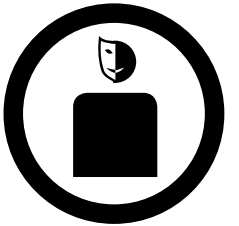
Inspired by Mehldau who created his icons inside of circles, probably chosen in reference to the icon referring to creative commons licences, this outer shape was chosen for the privacy icons as well. The rectangle lain over the circle indicates icons for data types. However, the type of outer shape is not finally determined yet. By now, we received user feedback that the circle is associated with something forbidden, as the circle often has this meaning with traffic signs - on the other hand round signs in blue colour indicate that something is allowed or compulsory. Others thought of triangular shapes as warning symbols. Therefore we took the decision of the round shape with rectangle content for some of the icons. Nevertheless, the design is still in progress.

The icon set approach developed in the second year is presented in the next sections. Some of the sections offer more than just one icon. One aim of the research in the second year was finding the best fitting icons. Therefore it was necessary to test them in a big variety to find out which of the approaches fits best and are best understood.

3.5.1 Icons for general usage

<u>Data type or purpose</u>		<u>Content</u>
<i>-Picture 1: Personal data</i>		Name and (physical) address are processed.
<i>-Picture 2: Sensitive data</i>	 	Special categories of data in the sense of Article 8 Data Protection Directive are processed. These include the processing of data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.
<i>-Picture 3: Medical data</i>	  	All kinds of data relating to data subjects' health can be expressed by these icons, e.g. prescription data or diagnostic data.

<p>-Picture 4: Payment data</p>		<p>Personal data related to financial issues and payment data.</p> <p>Data required for payment processes such as credit card or bank account number, tax ID and other billing information but not information used in anonymous payment methods.</p>
<p>-Picture 5: Data purpose: legal obligations</p>		<p>Includes all kind of data that has to be collected, processed and stored due to legal obligations.</p>
<p>-Picture 6: Data purpose: Shipping</p>		<p>Personal data that is necessary for the delivery of goods, e.g. delivery address, post office box, or packing station.</p>
<p>-Picture 7: Data purpose: User tracking</p>		<p>The data subject (user) behaviour is tracked by a website or webservice.</p>

		
-Picture 8: Data purpose: profiling	 	The data are used to create (group-)profiles of the data subjects. Note again that this is basically neutral and may even be to the benefit of the data subject, e.g., for matchmaking within a dating or friend-finder scenario.
-Picture 9: Storage		The data will be saved. An indication of the duration should be added.
-Picture 10: Deletion	 48 h	Data will be deleted. Retention time will be indicated employing a changing number on the right bottom of the icon unless a storage period has been indicated with the Storage-Icon already in direct proximity.
-Picture 11: Pseudonymisation	 	The data will be pseudonymised. This step is usually beneficial for the protection of the data subjects' privacy. However, the privacy policy should deliver details on who retains the data which enables a re-identification of the data subject and the conditions under which a re-identification may be carried out.

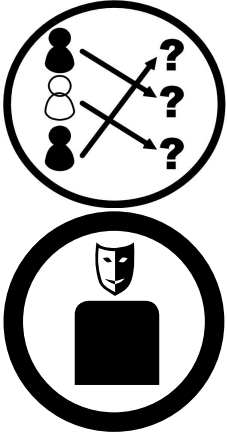
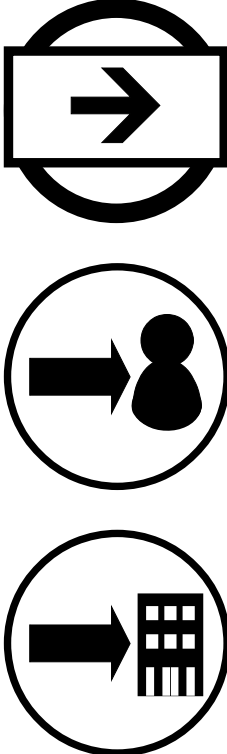
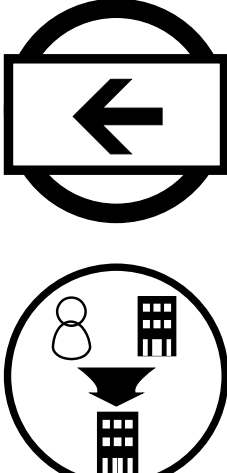

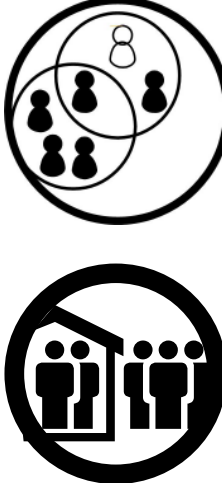
<p>-Picture 12: <i>Anonymisation</i></p>		<p>The data will be anonymised. The corresponding section in the privacy policy should declare within which processing stage the person related data will be anonymised. If possible, it should be indicated how well the anonymisation will exclude a direct link to the data subject, e.g., by giving the size of the anonymity set and informing on residual risks. The icon must not be used when the stored data still allows an identification of the subject or additional data are stored allowing a re-identification (see Pseudonymisation).</p>
<p>-Picture 13: <i>data</i> <i>disclosure</i></p>		<p>This symbol applies to any data processing step where data leaves the sphere of influence of the data controller. We suggest that this symbol is also applicable when data are processed by a data processor. While in the terms of the EC Data Protection Directive a data processor is not a third person and thus data are not “passed on”, it nevertheless duplicates the data and increases the number of persons handling with these data and thus constitutes at least an abstract increase of risk for the data subjects, who are neither able to verify the credibleness of the data processor nor to check on the controls and restraints the data controller is supposed to exercise over the data processor.</p> <p>The sign may be combined with a symbol for indicating groups of recipients or the specific name of the receiving entity.</p>
<p>-Picture 14: <i>data</i> <i>collection</i></p>		<p>Includes all kinds of personal data being collected by the data controller.</p>

Table 3. Icons for general use

3.5.2 Icons for usage in SNS

One of the icon approaches in the second year is to display data types and data purposes typical for SNS. People use SNS, because they want to share data. Thus, many steps of data disclosure, collection, handling and storing occur while using such services. Many users do not know who will get access to which information or what happens to their data on the server of the SNS. To inform the user about all these steps and to sensitise her for the privacy issues in a SNS, specific icons were developed. They should display important information for the user and strengthen her awareness. Therefore, the following icon sets for SNS have been developed and tested:

<u>Recipients</u>		<u>Content</u>
<i>-Picture 15: Friends</i>		In contexts where user groups are defined this icon symbolizes that the information will be distributed within such a group. In the field of social networks such a group may be referred to as friends. The group may be self-chosen (e.g., friends in a SNS, group in a SNS) or assigned by a third party (e.g., the department one works in).
<i>-Picture 16: Friends of friends</i>		Acquaintances such as friends of friends are useful for social networks. The groups need to be closer specified by the provider.






		
-Picture 17: Selected individuals	 	Displays the fact that only selected persons (of a bigger group like friends or friends of friends) will get access to specified data.
-Picture 18: public	 	All users of a given service or network or even the whole web community get access to the data. It is depending on the regulations on the access to the network this may come close to publishing the data (e.g., social networks where anyone may join).

Table 4. Icons for SNS usage

3.6 Test results

The icons displayed above have already been tested. A first test was performed by Karlstad University, a second one by CURE.

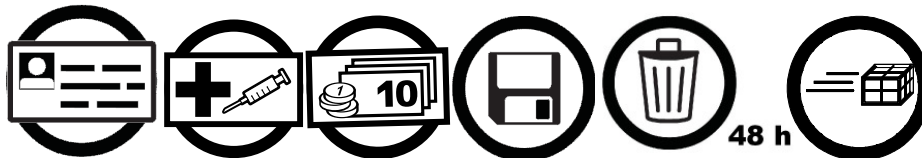
3.6.1 Test results from Karlstad University

The tests were conducted Karlstad University by Erica Nilsson in the form of paper mockup tests with 17 Swedish and 17 Chinese students. The tests were performed in English (for the Chinese students) and Swedish (for the Swedish students). The test was divided into two parts. Part 1 contained a general introduction, pre-test information and 5 pages of icons without headlines. Part 2 contained a shorter task introduction and 5 pages with icons with headlines. In the usability test the goal was to answer the questions:

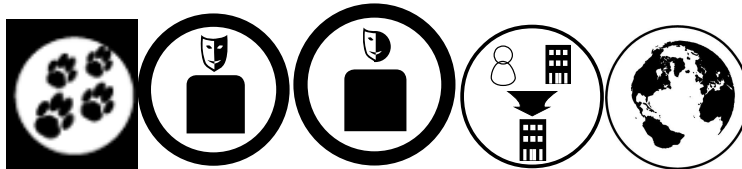
1. Are the icons understandable, clear and helpful?
2. Do the users understand the icons better with or without headlines?
3. Can the users contribute with better icons?

Only few of the tested students have been privacy aware before. To introduce them to the test, they got a short pre-test information about the idea behind the icons.

The test and its results gave a first hint of which icons seem to be well understandable and which require improvements. The results of the first part of the test showed that the students had a hard time understanding the icons without the headlines. Good icons seem to be the following ones for personal data, medical data, payment data, storage, deletion, and shipping.



The following icons for user tracking, anonymisation, pseudonymisation, data collection and the public as a recipient were not well understood and seem to require improvements.



It seemed that the differences between anonymisation and pseudonymisation were not apparent to the test persons at all.

The test also showed that it was important to take more than just one icon per purpose or data type for the test. Some of the icons for a specific purpose or data type were understood, whereas others for the same purpose or data type failed.

For instance, the following icon for medical data was well understood:



whereas, the following icon for medical data caused more confusions:



Many of the alternative icons for the same data type or purpose were however considered as equally good.

As a result the former work will be concentrated on those icons that were well accepted. Especially the icons for SNS usage therefore seem to be worth being adapted. The test showed - like it was mentioned above - that it is difficult to express the special purposes, data types or data transaction in SNS via icons. On the other hand, this also demonstrates the fact that many users have difficulties in understanding all aspects related to the processing of personal data within SNS. This shows the importance of visualizing those aspects.

The second part of the test showed that the students confirmed to a better understanding of the icons with headlines, but still had some problems. The meaning of "Pseudonymisation" and "Data disclosure" were not well understood by all students.

It was also obvious that the test persons had different understandings of the icons because of their cultural backgrounds. While Swedish test persons had for instance no problems in understanding the "post horn" as a shipping icon (see Picture 6 in Table 3), Chinese test persons did not understand it at all. The same appeared to the "paragraph" for the purpose "legal obligations" (see Picture 5 in Table 3. Icons for general use). This shows the fact that even those icons that are well understood in the western world are not necessarily as well understood by persons with an origin in another culture. A special challenge is to find icons that are well understood by all or most cultures.

At the end of the test, the students could give their ideas for icons. The following student approaches seemed to be worth being discussed:

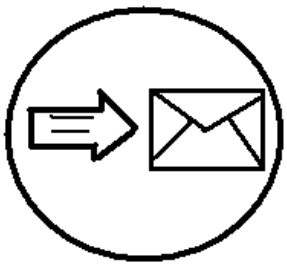

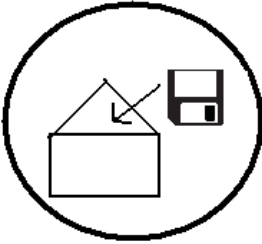
<u>Data purpose shipping</u>		
<u>Anonymisation</u>		
<u>Data importing</u>		

Table 5. Icon ideas of the test persons

The whole test also proved our assumption that displaying data transactions with icons seems to be more complicated than the displaying of data categories. A reason for this may be that many users are not familiar with data processing steps such as profiling, anonymisation, pseudonymisation or user tracking.

3.6.2 Test results from CURE

A second test of the icons by CURE with a bigger participation is still in progress. It has the same content but is built in a different way, so the test persons have more options to give their feedback. It is performed as an online test and the participants of this test are so far from Austria, Germany, The Netherlands and other European countries. The online test survey is available in German and in English⁹ and will may lead to more representative results, if a larger group of test users will participate in the test.

For the test, the icon sets have been amended with use-case-scenarios for a better understanding. The expected results of the CURE online test in combination with the tests conducted at Karlstad University will show which icons can be used in the current state, which will have to be improved and which ones will have to be removed from the icon set. The expected results will also ease the reduction of icons for the final sets of icons for SNS and for general use. Hence, the combined test results from CURE and Karlstad University will be the basis for further research and the final versions of the icon sets.

3.7 Icons for e-mail usage

Icons can be used to display many purposes and data types. They can also be used in many different scenarios. A first approach has been made to develop icons for usage in e-mails, as e-mail is one of the most frequently used mediums. In comparison to websites or SNS this medium is also less complex. For the purpose at hand e-mail may be treated as one to one communication as the sender chooses the recipients which also holds true also when sending copies or blind copies. Websites and SNS on the other hand usually broadcast their information to a multiple of usually unknown recipients or the entire web including spiders of search engines.

Researchers at Stanford University, PrimeLife members and interested individuals developed an icon set for e-mail. While this is still work in progress, interim versions are currently being published for discussion. The issues addressed by these icons were on the one hand similar to the purely privacy-related issues mentioned above. First of all, they included content-related issues. For example an e-mail might be confidential or should not be printed. It might also be possible to have e-mail content that may or even shall be shared with others. In the discussion between PrimeLife and Stanford, also differences in viewpoints on the understanding of privacy between US and Europe became apparent.

Another problem is the fact that e-mails do not offer that much space to display facts or purposes than websites do. They also usually do not include privacy policies which could be (partly) displayed by icons. If the e-mail includes a link to a written privacy policy, even less people would follow the link and read the policy than they would do so on websites. Thus, icons for e-mail usage have to display purposes and data types with reduced display options. It will also be difficult to explain icons in e-mails with mouse-over functionality or with a link. So the question is how to display icons with a lack of display options.

As e-mail is a text-based communication, the idea was to represent the icons only with letters and other symbols from the ASCII encoding scheme¹⁰ allowing mail clients to parse for the symbols and to represent them for visually impaired persons on Braille readers. A first suggestion for this is shown in:

⁹ See <http://survey.cure.at/index.php?sid=76747&lang=en>.

¹⁰ American Standard Code for Information Interchange, see: <http://en.wikipedia.org/wiki/ASCII>.

```

[o1] No print: Please don't print, keep it in digital form
[#]  No Archive: Please don't retain, delete within ____
[*]  Internal: Please only share with (common) friends
[<] Share: Please spread (under following cc-license...)
[/]  Off the record: Please do not tell anyone about this, or
[!]  Confidential: Please don't tell anyone this content.
[-]  Anonymous: Please don't attribute this content to me

```

Table 6. Example Icons set for e-mail usage in pure ASCII representation

It is suggested that also a graphical representation should be available:

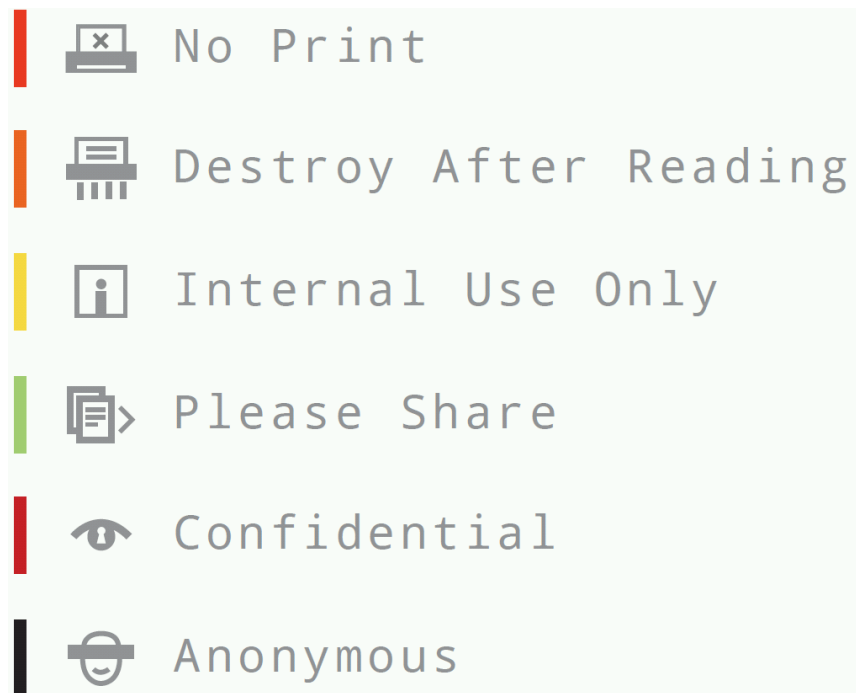


Table 7. Icons for e-mail usage graphical representation and colour codes
(Design of this representation by Andreas M. Brændhaugen licence: cc by-nc-sa)

The approach will be discussed with the interested public and further refined.

3.8 Future work

More detailed test results are expected after publication of this report. We expect that the results will point to further improvements and refinement of the icons but may also show which icons or underlying concepts should not be perceived further at all and thus should be dropped. These results will be presented in the final HCI research report.

The proposed icon sets together with a more elaborated syntax and semantics specification will require further refinement and testing.

At this point of time an outlook may be given on upcoming decisions to meet - based on the test results and on further testing:

- Outer shape of icons: At several project internal meetings the outer shape of the icons had been discussed. Inspired by Mehldau a circle had been chosen as outer shape for the privacy icons as well. The rectangle lain over the circle indicates icons for data types. As mentioned above, by now we received user feedback associating the circle with something forbidden as the circle often has this meaning for traffic signs. In the context of traffic signs a triangle has a warning function which disqualifies for the icons developed here as these should be free from any judgement regarding the processing steps.
- Colour codes have been discussed thoroughly and will be further considered and presumably tested in the context of e-mail icons.
- On the other hand it will prospectively be tested, which and how many icons can be combined to display certain aspects of privacy policies or data transactions. As it was discussed above, the icon sets shall be reduced to simplify them. Thus, it might be possible to display even more complex aspects with combined icons, so there won't be the necessity of having too many different icons. But the usage of combined icons must not confuse the user on the other hand. Therefore, the approach of reducing the icon sets will likely be combined with the approach of using combined icons to display data transactions.

Another design approach can be the creating of 3-dimensional or animated icons for a better visual appearance.

Furthermore, we can investigate whether icons should lead to the written policy via mouse-over functionality or whether there should be information about the icon in a first step and a link to the policy in a second step. This information could also be provided via mouse-over functionality or via direct-link.

After this, the next step will include matching the chosen icons to a selection of typical privacy policies in the web and offline world. One approach could be the implementation of icons in the web shop scenario to display the shop's privacy policy. This test could show whether the most important processing steps contained within the legal texts can be represented. Another approach could be the test of SNS icons in Clique, the privacy enhanced SNS developed within the PrimeLife project (see PrimeLife Deliverable D1.2.1).

A matching of the chosen icons with a full privacy policy could also provide the basis for further usability tests. This could show how the chosen models will be perceived and understood by users and whether some of the basic elements need further refinement.

Chapter 4

Multiple Steps Policy Management and Display Mockups - 2nd Iteration Cycle

Within PrimeLife’s Deliverable D4.3.1 “UI prototypes: Policy administration and presentation Version 1” a multi-stepped approach for UI-prototypes was described as ongoing research of a second iteration of the policy management and display mockups ([24] p. 43 et seq.). In this chapter, a brief summary of the two prototypes developed within the first iteration will be given including a description of the shortcomings and the user feedback that led to the development of a second iteration of the prototype (see 4.1). The second prototype and the requirements for its design will be described (see 4.2). This prototype has been tested and the test results will be described as well (see 4.3). The development ended in the coding of a third iteration for a check-out dialogue that will be introduced in chapter 5.

4.1 Past approaches and lessons learned

In PrimeLife D4.3.1, two versions for a UI prototype had been described. Both versions aimed at presenting additional information regarding the privacy of the customer (hereinafter: user) of a website or customer of a web shop (hereinafter: service provider) within the check-out dialogue. Check-out refers to the procedure of collecting information about the identity of the customer, an address for shipping the goods, payment information and possibly further data as well as the consent to use such data for purposes other than performing the contractual obligations. While the Data Protection Directive 95/46/EC provides a legal ground for data processing required for contractual obligations, this is not the case for other purposes such as for instance marketing purposes. This procedure is well known from online shops. However, in practice Online Shops often lack transparency with respect to the processing of personal data and providing privacy relevant information to the users.

4.1.1 Goals driving the development

Within PrimeLife Activity 4, it was found that some improvements to this procedure could be made that led to the development of this series of prototypes:

- The prototype displays the service provider’s privacy policy. A privacy policy describes how personal data will be handled by a service provider. Whenever a legal foundation for processing personal data is absent an informed consent of the user is required. For this, the user has to understand which terms and conditions regarding her personal data she agrees to, thus the policy must be understandable but nevertheless complete for being a valid legal basis for the data processing. The prototypes follow the multi-layered approach for displaying policies as suggested by the Art. 29 Working Party [3]. This will not replace a full written privacy policy to inform the interested user about details but the core information about which data will be processed for which purposes by which entity should be visible on a glance.
- The user should be able to predefine her interests regarding her privacy. Such a set of data is described as Privacy Preferences (“PrivPref” in short) (for details on the concept of Privacy Preferences see [25] p. 63 et seq.). The prototype should enable the user to display and manage such self-defined privacy preferences. The privacy preferences themselves will be managed by the user and stored on her local machine.
- The privacy policy and the user’s privacy preferences are matched and differences should be displayed by the prototype in an informative and rather non-alarming way. Previous tests with similar management prototypes from the PRIME project had shown that prominent warnings about mismatches may scare users and let them change their preference profile to more “generous” settings in order to get rid of the warnings.
- While a privacy policy must be kept rather general and applicable to all customers the checkout dialogue offers a possibility to display not only the data types that will be processed (e.g. name, birth date) but also the concrete data value transferred (e.g., Inga Vainstein, 21 December 1962). Besides enhancing transparency, displaying the data values gives an added value in particular to users utilising several partial identities and pseudonyms.
- While the data values are displayed, the user should also be able to change the values that will be transferred. This may include to choose another identity card or credential or to modify a text-field e.g. by picking another pseudonym or an alternative e-mail address instead of her real name.
- The user should be enabled to update her stored privacy preferences with such changed data on the fly or with any other modifications that she did (e.g. regarding the data processing purposes permitted by her) during the shopping transaction.
- As the policy display and administration system should assist user in administrating their partial identities and therefore has to process more personal information than needed by a service provider, the system should run at the user side under the control of the user.

A second iteration of the prototypes described in section 4.2 was developed, because the first iteration of the prototypes showed weaknesses in the user’s understanding of the information displayed. In particular, the second iteration aimed at clearly presenting the data required for an informed consent.

4.1.2 The first versions of the UI-prototype

This section will briefly introduce the prototypes of the first iteration to allow comparison and to illustrate the lessons learned from the user testing.

The first version of the mockup (prototype A) aimed at providing all necessary information at a glance. Therefore it had been attempted to provide all necessary information on a single page. At the same time it was intended to avoid that the user must scroll the page to see all information. For further details regarding these prototypes see [24] p. 29 et seq.

The users starts by choosing one of her pre-defined privacy preferences where loading the locally stored data into the form's fields. The purposes for which a certain piece of personal information may be used are displayed as checkboxes. The identity of the data controller (Nisses Books) is presented and a short indication on how the data will be processed is given. A screenshot of the prototype for the privacy preference "Only Minimal Data" is displayed below in Figure 3.

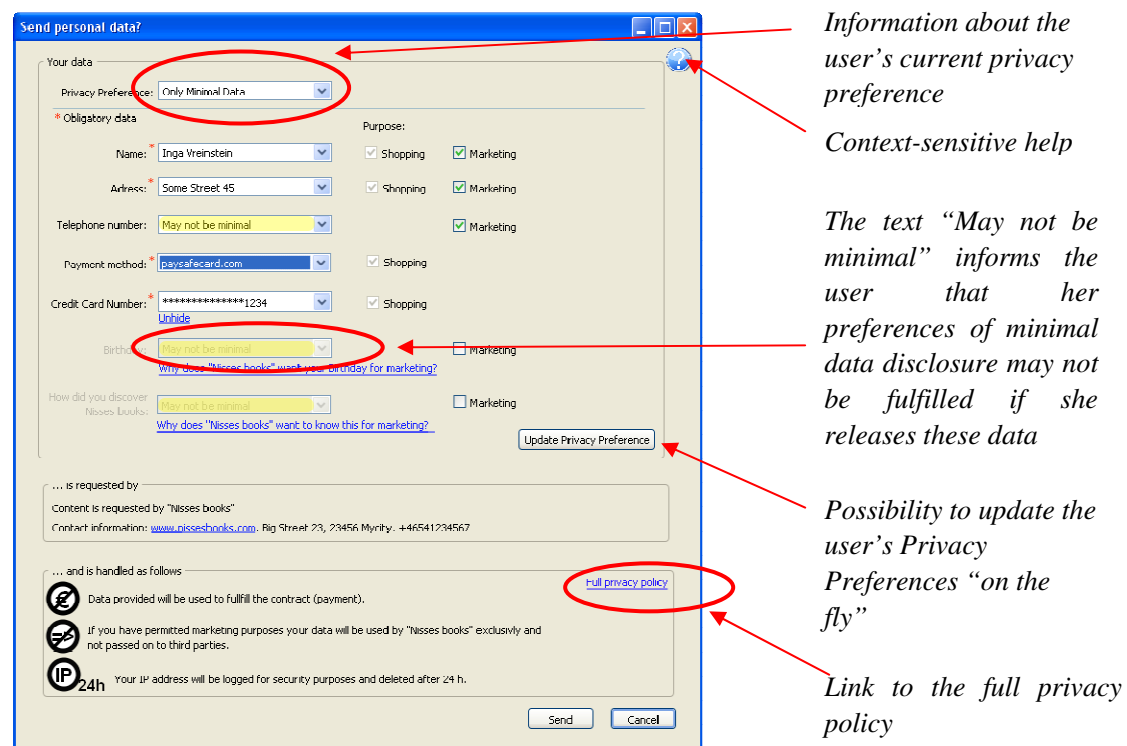


Figure 3. First UI Prototype for Policy Display and Management (prototype A)

While the approach shown in Figure 3 sorted the checkboxes for allowed purposes horizontally in a line with the data field, the alternative prototype developed by the PrimeLife Partner CURE placed them in a vertical order to allow better scalability of the page in case a transaction requires more data types or purposes (prototype B). This alternative prototype is shown in Figure 4 below:

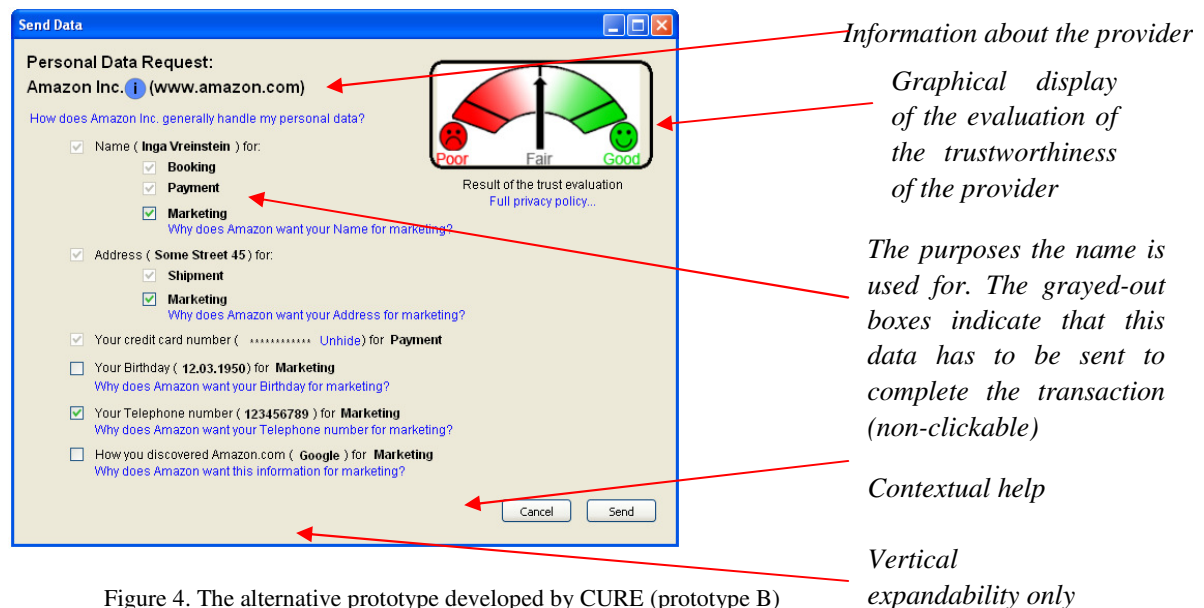


Figure 4. The alternative prototype developed by CURE (prototype B)

Detailed results of the user tests for both prototypes may be found in D4.3.1 [24].

4.2 Multiple steps approach - year 2 prototype

Testing of the first iteration's prototypes showed that the test persons noticed the possibility to use privacy preferences and had an idea, how these may be used to increase their privacy. The test persons also indicated that they would like to use privacy preferences to be alerted when a service requires more information than necessary.

While prototype A provided the users a better understanding about the use and disclosure of data than the alternative approach they criticised that the structure of prototype A was hard to understand. The test persons declared that they would wish additional help files which might have aided them to understand why certain checkboxes are available while others are greyed out.

As the users seemed to be better informed about which data is mandatorily asked for by the service provider by prototype A, it was decided to keep its table format.

Summing up the core critique of the users had been:

- Prototype A appears overcrowded.
- It was unclear, why certain checkboxes were unavailable.
- The result of the preference matching was not clearly understandable.
- It had been unclear, how the privacy preference can be changed or updated.
- Help aiding the users was not available.
- Not all information required for an informed consent as required by the data protection directive had been provided.

This led to the following aims for creating the second version of the prototype.

- To increase comprehensibility and transparency it was decided to try a multi-stepped approach having only few interactions per page reducing the complexity

for the user as only few decisions need to be met per page. A progress indicator should provide an overview of the steps.

- The pages are kept in a 4:3-type format to avoid the need for user to scroll the pages and to enable easy printing of the pages.
- Preference management is located within a dedicated step. All data stored in the local profile is displayed allowing the user to alter, update and save a stored preference before continuing with the selection on which data to send in the current interaction with a service provider.
- Help is provided by boxes that pop up when the mouse is hovered over a relevant object.
- A link to the service's full privacy policy is provided on all pages. Links to specific issues may be set where appropriate, e.g. jumping directly to the policy's section on data usage for marketing purposes.
- The result of the matching of the user's preference and the service's privacy policy is shown within an overview table right before allowing the data to be sent.
- The essential information for an informed consent should be provided within the prototype.

Step 1 Data processing steps

Step 1 presents an overview of the service's data requests and the purposes specified by the service provider. The purposes are structured in two sections - purposes that are mandatory to obtain the service and optional ones, for which the user may opt in. In the example in Figure 5 the shop "YourSHOP" asks for the user's data for payment and shipping purposes and for the optional purposes of analysing the user's interests for marketing and for using the contact information for marketing purposes.

Step one implements the presentation of necessary information for an unambiguously given, legally valid, informed consent for the data processing. To be valid, such a consent requires that the user is duly informed about the planned data processing including information about the name and address of the data controller, the purpose of the processing, the type of data processed, the identity of any data controllers to whom the data is disclosed to (see Art. 10 DPD, [26] Art. 2 para. 70; [27] § 4a BDSG para. 8). While the short information given in the prototype may not be sufficient to answer all questions, it concentrates on the essential information and allows the user to opt-in for additional purposes while further information laid down in the full privacy policy is just a click away, as it has been suggested by the layered policy approach introduced by the Art. 29 Working Party (cf. [3]).

Step 1 also acts as gatekeeper for the following steps. Optional purposes such as marketing may get a own step which will only be displayed, if the user opts for this specific purpose. Whether a checkbox agreeing to additional data processing may be pre-checked, depends whether an opt-out for the type of processing suffices or an opt-in of the user is legally required. This may differ depending on national legislation and the type of data in question.

PrimeLife Send Data Dialogue

Step 1: Data Processing Steps Step 2: Preference Management Step 3: Payment Step 4: Shipping Step 5: Marketing Step 6: Summary and Confirmation

YourSHOP Sample Street 4 support@yourshop321.com
London, UK +44 800 555 5535
EC4 SE8

requests your personal data for the following purposes:

To fulfill the purchase contract YourSHOP needs to process your data for:

- 1 payment of purchased item(s).**
In step 3 you will be able to choose your payment option and enter your data.
- 2 shipping of purchased item(s).**
In step 4 you will be able to choose your delivery option and enter your data.

In addition, you may consent to receive advertisement from YourSHOP

Please choose if you agree (your answer will not affect the transaction):

☐ YourSHOP may **analyze** my personal interests for marketing.
YourSHOP will store your personal interests. Based on your purchased and visited items your interests will be analysed with statistical methods to present you items you may be interested in. [Why does YourShop want to analyse my interests?](#)

☒ YourSHOP may **contact me for marketing purposes.**
If you agree to receive advertisement from YourSHOP you will be able to specify how YourSHOP may contact you in step 5. [Why does YourShop want to contact me for marketing?](#)

[click here](#) to see full privacy policy

Cancel **Next**

Figure 5. Step 1 Data Processing Steps

Step 2 Preference Management

Step 2 is dedicated to the preference management by the user. Within Step 2 (Figure 6) the prototype separates the management of the user's privacy preferences from the rest of the order process. The aim is to indicate that the data presented and changes done here are stored and processed locally on the user's client. The step starts with a selection of previously defined privacy preferences. All data stored within the respective PrivPref is displayed in the field below and may be changed according to the needs of the respective transaction. Changes to the PrivPref may be saved "on the fly" for future reference. Data fields in steps 3 and 4 will be continently pre-filled with the data selected here.

PrimeLife Send Data Dialogue

Step 1: Data Processing Steps **Step 2: Preference Management** Step 3: Payment Step 4: Shipping Step 5: Marketing Step 6: Summary and Confirmation

Here you can view and define your preferred PrivPref data set for this purchase at **YourSHOP** or decide to create a new one on the fly:

PrivPref Management
You can choose an existing or create a new PrivPref data set and the according fields will be prefilled in the following steps. At each step you can change the prefilled entries and later choose to update your PrivPrefs.

Minimal Data (for shopping)

View or adapt PrivPref entries or enter new

your address data may be used for	<input checked="" type="checkbox"/> payment	<input checked="" type="checkbox"/> shipping	<input type="checkbox"/> marketing
first name	street	city	zip code
Hannes	Dorfstr. 26	Buxtehude	21614
last name			country
Obermaier			Germany
further personal data may be used for	<input checked="" type="checkbox"/> payment	<input checked="" type="checkbox"/> shipping	<input type="checkbox"/> marketing
birth date	email address		
03.06.1973	hannes.obermaier@curi.at		
bank account data may be used for	<input checked="" type="checkbox"/> payment	<input type="checkbox"/> shipping	<input type="checkbox"/> marketing
bank name	account number		
Deutsche Bank	xx xx 17 09		
BIC code			
DEUTDE33HAN			
credit card data may be used for	<input checked="" type="checkbox"/> payment	<input type="checkbox"/> shipping	<input type="checkbox"/> marketing
credit card company	security number	card holder	expiration date
MasterCard	xxxx xxxx xxxx 4567	Hannes Obermaier	04 2014

[click here](#) to see full privacy policy

Back **Cancel** **Save** **Next**

Figure 6. Step 2 Preference Management

Step 3 Payment

Step 3 is dedicated for the selection of a payment method (see Figure 7). Depending on the data necessary for the transaction the required information will be pre-filled from the PrivPref chosen

during the previous step. The information that will be sent may still be altered at this stage. Information that is marked as mandatory by the service provider is marked with an asterisk.

Figure 7. Step 3 Payment - payment via credit card

Depending on the payment method, it may happen that no payment data at all will be transferred to the service provider, e.g. if the user opts for an anonymous payment service such as Paysafecard (see Figure 8), where the user is routed to the payment service at the end of the transaction and conducts the payment with an anonymous deposit.¹¹

Figure 8. Step 3 Payment - anonymous payment via Paysafecard

Step 4 Shipping

Within step 4 the shipping information is collected (see Figure 9). Depending on the chosen delivery method the necessary data is pre-filled in the lower section. Matching the policy of the

¹¹ See <http://www.paysafecard.com/ie/inform/> for more details on this anonymous payment method.

service provider with the privacy preferences “Minimal Data” of the user revealed that the information about the user’s birth date as well as the telephone number may not be necessary for this type of transaction. This mismatch is shown within the respective box, where the entry “many not be minimal” is written. Next to the request for the e-mail address, a link to the respective section of the privacy policy is placed where further information can be obtained on the purposes for which the e-mail address will be used by YourSHOP.

Figure 9. Step 4 - Shipping

A mismatch between the users PrivPref and the requested data is marked with yellow boxes and the explanation that this information may not be strictly needed for providing the requested service, which means that the request is not be consistent with the chosen PrivPref “Minimal Data”. However, the user is nevertheless able to fill in the data into the respective fields. This idea of indicating mismatches has been taken over from previous versions of the prototype and it was intended to compare it with the new approach shown in step 5.

Step 5 Marketing

Step 5 on marketing will only be displayed if the user indicated her consent to receiving marketing information from the data controller during step 1. Only if she allows her data to be used for marketing purposes the need arises to further specify in more detail the purposes and means of marketing that she want to permit.

Information necessary for the marketing methods where the user has opted for are marked with an asterisk. If such information has not been provided the user gets informed about this mismatch between the data provided and the chosen marketing methods with a question-mark shaped icon. Placing the mouse over the icon will provide context sensitive help by explaining why the mismatch occurred - and how to provide a remedy. In Figure 10 the user opted for receiving information via e-mail without providing her e-mail address. Consequently this mismatch may be remedied by taking away the checkmark in the box for electronic mail or by providing an address in the respective field.

PrimeLife Send Data Dialogue

Step 1: Data Processing Steps Step 2: Preference Management Step 3: Payment Step 4: Shipping **Step 5: Marketing** Step 6: Summary and Confirmation

Here you can specify how you agree to be contacted by **YourSHOP** and third parties for marketing purposes:

YourSHOP would like to contact you in the following ways (please pick options if you agree):

This step is presented to you because you indicated in step 2 that you agree to be contacted for marketing purposes. If you don't choose any option, you will not receive advertisement from YourSHOP.

☒ **postal mail to your invoice address**
☒ **electronic mail to your email address**
☐ **telephone marketing**

Depending on your chosen PrivPref some fields are prefilled, but can be changed

first name * Hannes last name * Obermaier email address * telephone number * marked items match above choice
street, no. * Dorfstr. 26 city * Buxtehude zip code * 21614 **Mismatch:** Based on your choice the service requests this data but you did not provide it.
birth date 03.07.1973 [Why](#) does YourShop want my birth date for marketing purposes?

[click here](#) to see full privacy policy **Back** **Cancel** **Next**

Figure 10. Step 5 Marketing

Step 6 Summary and confirmation

In step 6 all information will be summarised. A 2-dimensional matrix displays what data should be released for what purposes and offers the user a last possibility to select or unselect certain purposes and to send the collected data to the service provider. In addition the user can update her current privacy preferences with choices made during steps 3 to 5 or to save changes in a PrivPref thus changing the defaults or to retain the specific choices made under a new name for future reference and use.

Again, mismatches between the privacy preference and the user's current choice will be displayed together with an instruction how to resolve them. In Figure 11, the error shown in step 5 has not been rectified yet. The user may click on the question mark changing it to a checkmark allowing the e-mail address form the PrivPref to be filled in or by deselecting the option and thus to decline the service provider's request to use the data for contact marketing.

PrimeLife Send Data Dialogue

Step 1: Data Processing Steps Step 2: Preference Management Step 3: Payment Step 4: Shipping Step 5: Advertisement **Step 6: Summary and Confirmation**

Here you can view and change the data items that will be sent to **YourSHOP**

Data items	Payment	Shipping	Preference Analysis	Contact Marketing
Full Name	—	✓	—	✓
Street, No.	—	✓	—	✓
City, Zip code	—	✓	—	✓
Date of Birth	—	—	—	✓
E-Mail Address	—	—	—	?
Bank data	—	—	—	—
Credit Card	—	—	—	—

Preference Mismatch: Based on your choice the server requests this data but you did not provide it.
Check: provides email form PrivPref
Unchecked: unselects e-mail marketing

Your current selection deviates from your settings for the PrivPref „Minimal Data“.

☒ Yes, save PrivPref as

[click here](#) to see full privacy policy **Back** **Update PrivPref** **Send**

Figure 11. Step 6 Summary and Confirmation - mismatch e-mail missing

Likewise a mismatch with the PrivPref will be displayed. This is done in grey colour (see Figure 12). User testing done within the PRIME project indicated that users might be scared by warning signs and warning colours such as red and yellow with the result to change their profile in a way that warnings will not be indicated again. This, however, contravenes the use and purpose of the prototype and privacy preferences as such. Due to this and seeing the fact that the user has actively chosen to allow the transmission of data for marketing purposes during the previous steps, we opted for plain grey as an indicator for the mismatch. The mouse-over functionality offers help and explains the mismatch and the options how to resolve it. The green checkmark has been chosen for data that will be sent that is necessary for the transaction.

PrimeLife Send Data Dialogue

Step 1: Data Processing Steps Step 2: Preference Management Step 3: Payment Step 4: Shipping Step 5: Advertisement **Step 6: Summary and Confirmation**

Here you can view and change the data items that will be sent to **YourSHOP**

Data items	Payment	Shipping	Preference Analysis	Contact Marketing
Full Name	—	✓	—	✓
Street, No.	—	✓	—	✓
City, Zip code	—	✓	—	✓
Date of Birth	—	—	—	✓
E-Mail Address	—	—	—	?
Bank data	—	—	—	—
Credit Card	✓	—	—	—

Preference Mismatch:
You provided this information, but this exceeds the profile „Minimal Data“.

Your current selection deviates from your settings for the PrivPref „Minimal Data“.

☒ Yes, save PrivPref as

[click here](#) to see full privacy policy

Back Update PrivPref Send

Figure 12. Step 6 Summary and Confirmation - mismatch with privacy preference

4.3 User feedback on the second iteration cycle

The prototype introduced above has been tested with guided usability tests and post test interviews at Karlstad University in December 2009 to receive first feedback. Test manager was Maria Lindström. Five test persons participated, which who all students at Karlstad University. The test plan and questionnaires that were used are published in Appendix A.

As mentioned above, Nielsen [28] points out that if several iterations of mockup developments/improvements and tests are planned, it will be sufficient to have 5 users for each iteration. We have also decided to do a series of iterations of mockups redesigns for our policy mockups and tested them with 5 test persons in each iteration round.

The test results as well as an interview with the owner of an online shop held at ULD lead to the development of a third iteration of the prototype which will be introduced in the chapter 5 below.

4.3.1 Test setup and conduction

The main objective of the test had been to collect user opinions and feedback about the prototype. It should be determined, whether the test persons perceived the stepped approach better than the one step approaches chosen during the first iteration.

The test leader gave the test persons an introduction and the assignment telling them that they will be ordering a book at the YourSHOP website. They were told that after confirming the content of the virtual shopping cart, the PrimeLife prototype is activated and were asked to allow the shop

using their data for marketing purposes. The test persons were encouraged to explain what they saw on the screen and what they thought that the software did. For each step specific questions or tasks had been asked or were assigned respectively.

4.3.2 Test results

The test persons had some general comments regarding the prototype which will be presented before listing the specific comments for each of the six steps.

Again, all participants liked the idea of privacy preferences but found it confusing. They asked for a better visualisation of the concept. While it was welcomed that the interaction was split into different steps, the redundancy was criticised. Also one person said that she would not like to go through all steps every time that she shops online. This shows that it was not possible for us to convey the information to the test persons that step 2 actually takes workload from them just as a form filler would do and that a user only needs to review and adapt previously entered data or may just rush through the steps as things are pre-filled and pre-decided already once a PrivPref has been selected.

In general, the test persons liked the multiple-steps approach and the arrow on top of the page indicating the progress throughout the procedure. Step 6 was well perceived, as the table with the options for selecting purposes to allow was easy to use.

Nearly all participants considered the prototype “messy” while referring to the rather crowded steps and the sometimes tiny print. It was asked for a clearer structure and presentation of the respective points as well as a reduction of the information presented to a minimum.

Step 1

Task: “Make your settings in step 1 and try to explain what your setting means to you”

Within step 1 four of the five test persons tried to unselect the checkbox for marketing. The circled numbers 1 and 2 in the upper box puzzled the participants and they also attempted to click on the circles. Also the difference between the content of the two boxes were unclear to the participants. One person stated that she likes to buy a book and the shop may ask for permissions regarding marketing at the end. This questions the approach of step one having a gatekeeper function for any optional purposes which would be reflected in additional steps that would either be shown when opted for such a service or hidden from the user. One person would read headlines but the boxes are missing such headlines. It was suggested to have a shorter name for the step such as “purposes”.

Step 2

Task: The test persons were asked where the presented information was stored (e.g. where it comes from). They were also asked what the checkboxes mean and what information they refer to.

Most participants guessed correctly that the data would have been entered by themselves during the installation of the client software. However, this was not really clear and one person was confused that YourSHOP knew so much information about her.

Most participants could not allocate that the boxes belong to the rows with the headlines. One person consequently suggested inverting the table thus having the checkboxes in a vertical order.

Step 3

Task: The users were asked to choose credit card as payment method. They were then asked to explain where the credit card data came from.

The users were aware that the information has been entered by them earlier. One person was confused as she had just seen the information in the previous step. Further, the third step did not appear so crowded and messy than the second one. However, it was asked why the upper and lower parts are separated by boxes when obviously the radio button is related to the information displayed below.

Step 4

Task: The participants should keep the current delivery choice. They were asked to explain the difference between the two yellow coloured boxes.

One person understood the concept that the yellow colour indicates that this referred to information that should not be revealed according to the chosen privacy preference and that the fields differed in respect to being mandatory or not. The yellow fields were confusing for four of the five participants. The yellow colour implies that “something is wrong” or specifically important.

It was unclear for one person how to make the colour disappear. Again, it was mentioned that the content of the upper and lower boxes belong together and should not be separated optically with the boxes.

Step 5

As in step 4 the participants were asked to leave the choices as they were and to explain the meaning of the question mark. As four of the participants unselected marketing during step 1, this step had not been shown to them. The remaining participant did not understand the question mark or how to make it disappear.

Step 6

Task: The participants were asked why they are prompted to save a new PrivPref. They were further asked to choose between saving a new PrivPref or updating an existing PrivPref.

Some test persons opted for updating. One person thought that she must update before sending the information. Only one person wondered whether the profile is specific for YourSHOP or specific for the preference “Minimal Data”. She therefore understood that the tool could be used as a mean to operate with different partial identities towards different service providers, but was confused by the layout of the page.

4.4 Conclusions for a third iteration

Some of the main usability issues that need to be addressed can be summarised as follows:

- While in principle, the users liked a multiple steps approach, six steps in total were perceived as too many. Especially, the first two steps (“Data processing steps” & “Preference Management”) were not appreciated.
- The “Update PrivPref” option was difficult to understand users tend to update/save too quickly without understanding the implications.
- Mismatches need to be better displayed.

Overall, the test results led us to the following conclusions for the next iteration of the prototype:

- As the two-dimensional table presentation of what types of data will be released for what purposes was in general well perceived, the next iteration should keep the 2-dimensional table with the data types and preferably also display the data values that will actually be sent.
- To keep redundancy of entries low, the table should be the core of the prototype giving possibility to view and alter data types, permitted purposes and also displaying all recipients. Also mismatches could be visualised within the table and explained in a box placed nearby or in a mouse-over action.
- A menu for configuring and managing Privacy Preferences should only optionally be available for the advanced users.
- Accessibility should be increased. In particular readers and other aids for the visually impaired should be able to parse such pages as well.

In addition the PrimeLife team at the project partner ULD had an interview session with a local service provider owning and running a web shop. Core finding of the interview had been that a shop loses customers with every step to go during the checkout process and that the technology suggested with the prototype could only be successful when service providers support it as well which is unlikely to happen when the normal checkout procedure is prolonged by several stages. This encouraged PrimeLife to cut down on the number of steps to get also the support of possibly interested service providers.

Chapter 5

Policy Management & Display Mockups –3rd Iteration cycle

The PrimeLife checkout (PLC) user interface aims at supporting the user in enforcing her privacy preferences in an online purchase process. The user can choose how much privacy protection she wants, and the system visualises what shipping and payment methods are matching with her needs or why the selected methods are not suitable for the protection level chosen. The interface displays which personal data will be transferred to whom for what purposes in a user friendly way. In most online shops this information can only be retrieved by reading the shop's full privacy policy, i.e. no user-friendly overview what data will be transferred to whom for what purposes is provided. As all the other policy management & display mockups presented in the deliverable, also the PLC approach tries to specifically address this problem of a user-friendly and more transparent policy display.

5.1 Description

Every additional click increases the risk that the shop user terminates the session before finalising her purchase. As reported in the previous chapter, also our usability tests of the Multiple Steps “Send Personal Data” Dialogue showed that end users were of the opinion that 5 steps were too many. Seven steps are needed to buy something at Amazon.com as visualised in Figure 13. The problem for the user is that she has no knowledge if the data that she entered are finally accepted by the system.

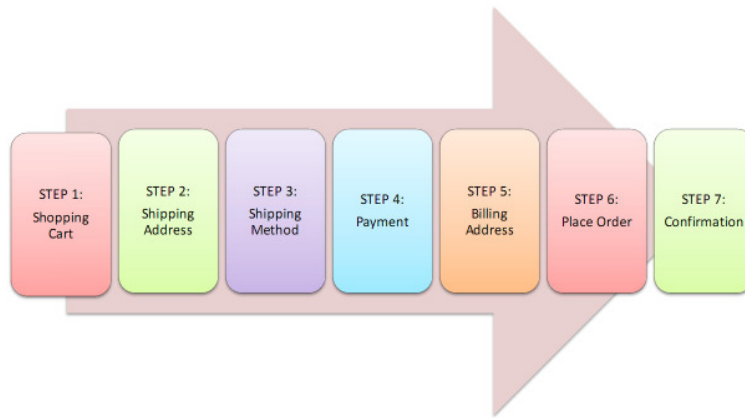


Figure 13. Steps solution by Amazon.com

A typical scenario is that the user has to enter data, click next, find out what data was rejected for which reason by the system, correct the problem and try it another time.

This can be very annoying for the user. Such kind of dialogue procedure has its roots from the times before Ajax¹² was in use. The whole processing in the WWW was done by the servers and the browsers could not run code such as JavaScript¹³.

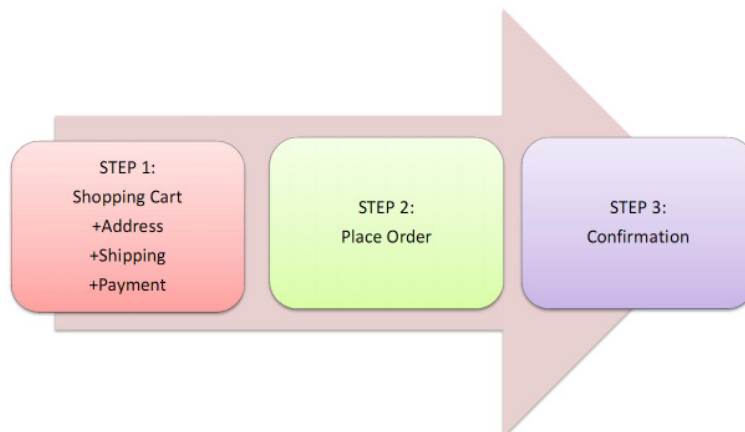


Figure 14. PLC tree steps solution

The PLC solution chooses a different approach. The objective is to collect all necessary data in a single step. In the moment that the user enters the data, PLC will check the validity of the data. This step is performed in the realm of the user's browser without transferring any data to the server. The user gets instant feedback if the entered data is valid and fulfilling all requirements or if she has to correct something.

¹² Asynchronous JavaScript and XML (Ajax) is a method for web pages to transfer data between browser and server after the page has been loaded. The advantage is that the webpage does not to be fully reloaded to react on users input. Just a small part of the webpage needs to be transferred. The user gets instant feedback after manipulating elements of the webpage.

¹³ JavaScript is a scripting language that can be interpreted by modern web browsers. It enables web developers to embed small pieces of software into web pages that will be executed by the web browser to make web pages react on user input without reloading the webpage.

The resulting steps are shown in Figure 14 – the procedure just needs two steps for the purchase, the user gets instantaneous feedback, and may correct her data if needed.

5.1.1 Three Step design

As shown in Figure 14, the PLC is divided into only three steps in total in order to reduce the amount of clicks the users have to do to finish to their purchase. The different steps will be described in this subsection.

The usual solution is that after every step the data of the user is transferred to the webshop. The user has no control what the webshop does with this data. One popular way of misusing data is to request a score value from credit agencies without the user's consent and selecting the offered payment methods by the result of the score.

The major advantage of the PLC solution presented in this chapter is that all data will only be transferred at the end of the process in one bunch and only if the user finishes the whole process. The webshop cannot score the customer and select payment methods by the score value without the user's consent. If the user cancels the process at any time, no data will be transferred to the server.

5.1.1.1 Step 1 - Shopping Cart

In the first step, the user has to enter all necessary data to perform the purchase as shown in Figure 15. She is informed that she is in step one out of three and that no data will be transferred to the webshop until she confirms the data transfer in the next step. The user will also get a view on her current shopping cart with the option to finally change the amount of the selected items.

Step 1: Shopping Cart → Step 2: Summary → Step 3: Confirmation

No data within the grey area will be transferred until you click "Order and Transfer Data" in next Step!

My Privacy Settings
☒ Nearly Anonymous [View & Customize](#)
☐ Few Data [View & Customize](#)
☐ Don't Care [View & Customize](#)
[Insert Privacy Settings](#)

Shopping Cart

Items	Quantity	Price per item	Total price
Terminator Salvation DVD - BBFC 18	2	9.95 €	19.90 €
Cerazette mini pill	3	31.39 €	94.17 €
DVD Player	1	35.30 €	35.30 €

Shipping
☐ DHL parcel - uninsured + 3.90 €
☐ Hermes parcel + 4.00 €
☐ DHL parcel - insured + 6.00 €
☒ DHL parcel to parcel station + 3.50 €

Payment
☒ PaySafeCard + 0.00 €
☐ Visa + 0.99 €
☐ prepay bank transfer + 0.00 €
☐ pay on delivery + 0.00 €

Sum
 Without Tax 3.90 €
 Tax 4.00 €
 Total 4.00 €

Data to Transfer
to Webshop (Purchase):
 Address Line 1 : Parcelstation 101
 Postcode : 12345
 City : Mycity
 Country : EU
 E-mail : John@doe.eu

 Data will be processed and stored for the purpose of:
 • Tax - 10 years
[Detailed Privacy Policy](#)

to DHL (Shipping):
 Address Line 1 : Parcelstation 101
 Address Line 2 : 12345678
 Postcode : 12345
 City : Mycity
 Country : EU
 E-mail : John@doe.eu

 Data will be processed and stored for the purpose of:
 • Tax - 10 years
 • Delivery - 7 days
[Detailed Privacy Policy](#)

My Data
 All fields marked with an "*" are mandatory.

		Webshop (Purchase)	DHL (Shipping)	PaySafeCard (Payment)	Webshop (Statistics)	Webshop (Special Offers)
First Name	John	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Last Name	Doe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 1	Parcelstation 101	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 2	12345678	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Postcode	12345	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
City	Mycity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Country	EU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail	John@doe.eu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone Number	+494319881200	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card No.	1234 5678 9012 3456	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Expiry Date	1/2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Verification Code	123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Privacy Settings Matching

MATCH ✓

User Settings Matching

MATCH ✓

[← Return to Shop](#)
[Next Step: Summary →](#)

Figure 15. Step 1: Shopping Card

5.1.1.2 Step 2 – Summary

In the second step, the PLC will display all the data that have been collected in the first step again in the same setup without the option to manipulate it as shown in Figure 16. The user has the opportunity to save the data that she entered in step 1 plus information to whom the data may be transferred for what purposes to her privacy settings. She can check if all data that she entered are

correct and confirm the purchase and data disclosure by clicking on the “Order and Transfer Data →” link or go back and make changes by clicking on “← Return to Shopping Cart”.

This step is redundant and could be left out, but many users expect to take a final persistent view on their purchase and on what data will be transferred to whom for what purposes before finally confirming the purchase and data transfer. This is achieved by the second step.

Step 1: Shopping Cart → **Step 2: Summary** → Step 3: Confirmation

No data within the grey area will be transferred until you click "Order and Transfer Data" on this page!

My Privacy Settings
 Nearly Anonymous
[Safe Privacy Settings](#)

Shopping Cart

Items	Quantity	Price per item	Total price
Terminator Salvation DVD - BBFC 18	2	9.95 €	19.90 €
Cerazette mini pill	3	31.39 €	94.17 €
DVD Player	1	35.30 €	35.30 €

Shipping
 DHL parcel to parcel station €3.50

Payment
 PaySafeCard €0.00

Sum
 Without Tax 3.90 €
 Tax 4.00 €
 Total 4.00 €

My Data

		Webshop (Purchase)	DHL (Shipping)	PaySafeCard (Payment)	Webshop (Statistics)	Webshop (Special Offers)
First Name	John	-	-	-	-	-
Last Name	Doe	-	-	-	-	-
Address Line 1	Parcelstation 101	✓	✓	-	-	-
Address Line 2	12345678	-	✓	-	-	-
Postcode	12345	✓	✓	-	-	-
City	Mycity	✓	✓	-	-	-
Country	EU	✓	✓	-	-	-
E-mail	John@doe.eu	✓	✓	-	-	-
Phone Number	+494319881200	-	-	-	-	-
Credit Card No.	1234 5678 9012 3456	-	-	-	-	-
Credit Card Expiry Date	1/2014	-	-	-	-	-
Credit Card Verification Code	123	-	-	-	-	-

Data to Transfer
to Webshop (Purchase):
Address Line 1 :
 Parcelstation 101
Postcode : 12345
City : Mycity
Country : EU
E-mail : John@doe.eu

 Data will be processed and stored for the purpose of:
 • Tax - 10 years

[Detailed Privacy Policy](#)

to DHL (Shipping):
Address Line 1 :
 Parcelstation 101
Address Line 2 :
 12345678
Postcode : 12345
City : Mycity
Country : EU
E-mail : John@doe.eu

 Data will be processed and stored for the purpose of:
 • Tax - 10 years
 • Delivery - 7 days

[Detailed Privacy Policy](#)

[← Return to Shopping Cart](#)
[Order and Transfer Data →](#)

Figure 16. Step 2: Summary

5.1.1.3 Step 3 – Confirmation

In the third step, the PLC confirms the purchase as shown in Figure 17. It also notifies the user that the data that she has entered have been transferred to the providers listed in the “My Data” field and in the right bar. The user has again the opportunity to save the selected privacy settings for future use and reference.

Step 1: Shopping Cart → Step 2: Summary → **Step 3: Confirmation**

Thanks for your order!
Your data has been transferred to the recipients listed in the right bar.

My Privacy Settings
Nearly Anonymous
[Safe Privacy Settings](#)

Shopping Cart

Items	Quantity	Price per item	Total price
Terminator Salvation DVD - BBFC 18	2	9.95 €	19.90 €
Cerazette mini pill	3	31.39 €	94.17 €
DVD Player	1	35.30 €	35.30 €

Payment
PaySafeCard €0.00

Shipping
DHL parcel to parcel station €3.50

Sum
Without Tax 3.90 €
Tax 4.00 €
Total 4.00 €

My Data

		Webshop (Purchase)	DHL (Shipping)	PaySafeCard (Payment)	Webshop (Statistics)	Webshop (Special Offers)
First Name	John	-	-	-	-	-
Last Name	Doe	-	-	-	-	-
Address Line 1	Parcelstation 101	✓	✓	-	-	-
Address Line 2	12345678	-	✓	-	-	-
Postcode	12345	✓	✓	-	-	-
City	Mycity	✓	✓	-	-	-
Country	EU	✓	✓	-	-	-
E-mail	John@doe.eu	✓	✓	-	-	-
Phone Number	+494319881200	-	-	-	-	-
Credit Card No.	1234 5678 9012 3456	-	-	-	-	-
Credit Card Expiry Date	1/2014	-	-	-	-	-
Credit Card Verification Code	123	-	-	-	-	-

Data Transferred to Webshop (Purchase):
Address Line 1 : Parcelstation 101
Postcode : 12345
City : Mycity
Country : EU
E-mail : John@doe.eu

Data will be processed and stored for the purpose of:

- Tax - 10 years

[Detailed Privacy Policy](#)

to DHL (Shipping):
Address Line 1 : Parcelstation 101
Address Line 2 : 12345678
Postcode : 12345
City : Mycity
Country : EU
E-mail : John@doe.eu

Data will be processed and stored for the purpose of:

- Tax - 10 years
- Delivery - 7 days

[Detailed Privacy Policy](#)

Figure 17. Step 3: Confirmation

5.1.2 Elements of the PLC

In this section, we provide a short description of the components of the PLC..

At the top of the PLC user interface, there an overview of all steps, where the current step is displayed in bold and underlined

In the box below the steps, the user gets the information that no personal data entered within the grey area will be transferred until the user finally clicks “Order and Transfer Data”. In the last step, this box will show the confirmation that the data have been transferred to the recipients listed in the right bar.

My Privacy Settings

An important part of the PLC is the “My Privacy Settings” box shown in Figure 18, where the user selects her preferred Privacy settings. There are three predefined settings available: “Nearly anonymous”, “Few Data” and “Don't care”. In addition, there is a field for the user to insert her own privacy settings with the help of a policy editor.

The names of the privacy settings should indicate how much personal information the user is willing to disclose:

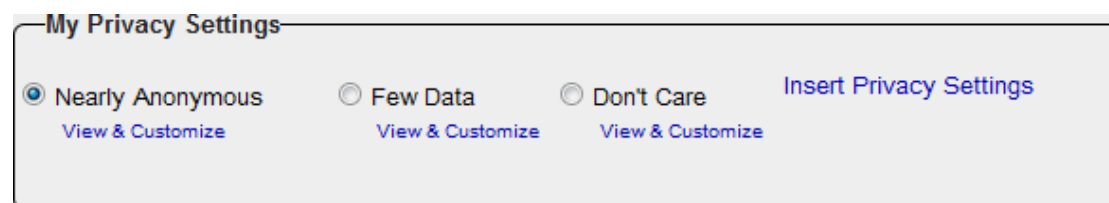


Figure 18. My Privacy Settings

- “Nearly Anonymous” is the most restrictive setting, where the user does not want to reveal any personally identifiable information, i.e. she desires to act anonymously. As for web transactions, real anonymity is hard to measure and guarantee, we call the settings “Nearly anonymous” to prevent that more is promised than what can actually be achieved.
- With “Few data” the shop, the shipping company and the payment provider will only get the data needed to perform the transactions.. Additional purposes for data collection and data usage such as marketing are generally not allowed with this setting.
- The settings “Don't care” disable all restrictions. The user can configure to disclose her data without being warned by the system that the webshop’s privacy policy does not match with her privacy settings.

Payment and Shipping

The “Payment” or “Shipping” boxes show a list of payment and shipping provider. The user can select a provider as shown in Figure 19.

Payment

<input checked="" type="radio"/> PaySafeCard	+ 0.00 €
<input type="radio"/> Visa	+ 0.99 €
<input type="radio"/> prepay bank transfer	+ 0.00 €
<input type="radio"/> pay on delivery	+ 0.00 €

Figure 19. Payment provider selection

My Data

The “My Data” box shown in Figure 20 contains text fields, where the user can enter personal data requested by the service provider. It also contains a matrix with which the user can select with checkboxes which data should be transferred to whom for what purposes.

My Data

All fields marked with an "*" are mandatory.

		Webshop (Purchase)	DHL (Shipping)	PaySafeCard (Payment)	Webshop (Statistics)	Webshop (Special Offers)
First Name	John	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Last Name	Doe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 1	Parcelstation 101	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 2	12345678	<input type="checkbox"/>	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Postcode	12345	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
City	Mycity	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Country	EU	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail	John@doe.eu	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone Number	+494319881200	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card No.	1234 5678 9012 3456	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Expiry Date	1/2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Verification Code	123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Privacy Settings Matching

MATCH ✓

User Settings Matching

MATCH ✓

Figure 20. My Data field including Matching results

Text fields

In the text fields the user can enter the personal data requested. The fields are grey coloured if data for that respective field are not requested, yellow if the information in the field is necessary for completing the transaction but not inserted yet or incorrectly filled in, and white if the data are necessary and correctly filled in.

Checkboxes

The checkboxes are arranged in a matrix with data fields as rows and the data controllers/purposes as columns. Every checkbox symbolises if information from the customer is transferred to a data controller or not. A checkbox has two binary states. The checkbox can be “enabled” or “disabled”,

which means that the checkbox status can be modified by the user (enabled) or not (disabled). A checkbox can also be checked or unchecked. A checked checkbox means that the data inserted in the data field of the respective row are sent to the data controller in the respective column for the specified purpose. If the checkbox is unchecked, the data won't be transferred.

If there is an asterisk next to a checkbox, the data field is mandatorily requested by the data controller. To perform the purchase successfully, the user has to give her consent to transfer the information by checking the checkbox next to the asterisk or select a different data controller if possible, e.g. a different shipping provider who does not request that data. Otherwise there will be a mismatch.

My Data
All fields marked with an "*" are mandatory.

Webshop (Purchases)
DHL (Shipping)
Paycard (Payment)
Webshop (Statistics)
Webshop (Special Offers)

Field	Value	Webshop (Purchases)	DHL (Shipping)	Paycard (Payment)	Webshop (Statistics)	Webshop (Special Offers)
First Name	John	<input type="checkbox"/>	<input type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Last Name	Doe	<input type="checkbox"/>	<input type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 1	Parcelstation 101	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 2	12345678	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Postcode	12345	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
City	Mycity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Country	EU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail	John@doe.eu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone Number	+494319881200	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card No.	1234 5678 9012 3456	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Expiry Date	1/2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Verification Code	123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Privacy Settings

MISMATCH X

Your Privacy Settings do NOT match with the DHL Privacy Policy.

Mismatches:

- Your **First Name** is requested for **Shipping** purposes.
- Your **Last Name** is requested for **Shipping** purposes.

User Settings Matching

.....

Figure 21. My Data field with a "Privacy Settings" mismatch

Matching

The PLC matches the "selected "Privacy Settings" with the "Privacy Policy" of the different data controllers. The choice of the "Privacy Settings" determines the states of the checkboxes in the matrix. The "Privacy Policy" of the data controllers is compared with states of the checkboxes in the Matrix. If both are matching there will be a "MATCH ✓" in the box on the right side of the Matrix, otherwise there will be a "MISMATCH ✗".

If the mismatch can be resolved by the user without changing her Privacy Settings, there will be an orange exclamation mark "!" on the right side of the checkbox where the mismatch is located and the mismatch will be displayed in the "User Settings Matching" box as shown in Figure 22. If the user has to change the Privacy Settings in order to resolve the conflict, the exclamation mark will be red and the mismatch will be displayed in the "Privacy Settings Matching" box as shown in Figure 21. The details of the mismatches are displayed in the boxes on the right side of the matrix.

Colour-blind people can distinguish the different mismatches with the help of the text in the boxes.

The user can only proceed with the shopping transaction if there are no mismatches.

My Data

All fields marked with an "*" are mandatory.

Webshop (Purchase)
DHL (Shipping)
Paysafecard (Payment)
Webshop (Statistics)
Webshop (Special Offers)

First Name	John	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Last Name	Doe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 1	Parcelstation 101	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Address Line 2	12345678	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Postcode	12345	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
City	Mycity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Country	EU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail	John@doe.eu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone Number	+494319881200	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card No.	1234 5678 9012 3456	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Expiry Date	1/2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Verification Code	123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Privacy Settings Matching

MATCH ✓

User Settings

MISMATCH ✗

DHL needs the following fields:

- Your **First Name** is requested by for **Shipping** purposes.
- Your **Last Name** is requested by for

Figure 22. My Data field with a "User Settings" mismatch

Data to Transfer

to Webshop (Purchase):

Address Line 1 :
Parcelstation 101

Postcode : 12345

City : Mycity

Country : EU

E-mail : John@doe.eu

Data will be processed and stored for the purpose of:

- Tax - 10 years

[Detailed Privacy Policy](#)

to DHL (Shipping):

Address Line 1 :
Parcelstation 101

Address Line 2 :
12345678

Postcode : 12345

City : Mycity

Country : EU

E-mail : John@doe.eu

Data will be processed and stored for the purpose of:

- Tax - 10 years
- Delivery - 7 days

[Detailed Privacy Policy](#)

Figure 23. "Data to Transfer" box

Overview of data transfer

One main objective of PLC is to visualise in a user-friendly manner what will be done with the data disclosed by the user. This is expressed by a list of all data the user has entered which shows all involved data controllers with all data fields (attributes) and field content (attribute values) that will be transmitted if the purchase is completed. The list is updated in real-time so that the user can immediately observe consequences of all her changes. For this, the “Data to Transfer” box on the right side of the user interface displays for each data controller what data will be disclosed, for what purposes and what will be the data retention periods for the respective purposes. Besides, links to the full privacy policies of the data controllers are provided to comply with the Art. 29 Working Part recommendation on Multi-layered privacy policies [3].

5.2 Usability test

The usability tests were performed in May 2010 by Staffan Gustavsson with five participants. As mentioned above, according to Nielsen [13] this is enough during design cycles as several features of the designs will reappear during late cycles in the design process.

5.2.1 Test design

The test was designed as a semi-structured interview with a test scenario where the test users were asked to purchase products as a starting point, see Appendix B. The semi-structure was chosen since the different parts of the GUI needed to be discussed and examined in detail, while the interview needs to follow the participants’ way of interacting with the mockups.

In the test participants were told that they had put these items in the shopping cart and now wanted to complete the purchase. They were then given information about a person called “Anders Andersson” and told to act as him while working with the mockup.

5.2.2 Test participants and execution

The participants were all students at Uppsala University between 20 and 26 years old, three were males and two were females.

The test was conducted in the university’s corridors. Students who were studying on the campus were asked if they would like to participate and were given lunch coupons to the university restaurant as a compensation for participating.

The tests all took approximately 30 minutes.

5.2.3 Results

The results given below are divided into the different parts of the GUI that the interview focused on.

5.2.3.1 Privacy settings

The participants generally seemed to understand the meaning of the privacy settings, they all understand that it is concerned with how much information one will disclose. What they do not understand is the different meanings of how much information will be given away and for what purpose.

“Nearly anonymous” was explained as *“the information I send cannot be connected to me directly”, “seems like the most secure one”, “only the essential data is sent” and “I do care so I choose this one”*.

“Few data” was explained as *“I can choose which information to send”, “does not know what this mean”, “the company will be responsible for not treating my data in a ‘bad’ manner” and “probably means more to fill in so I choose nearly anonymous”*.

The “don’t care” option was explained as *“I send more information than the other two and the company can do whatever they want with it”, “all data that can be sent will be sent and the company will do whatever they want with it” and “all data possible will be sent”*.

All participants chose “nearly anonymous” since they believed that this was the most secure option and the one they felt most comfortable with. This choice explains some of the problems the participants had later with understanding the “May Data” field and information about related preference settings/ user settings (Mis-) matches, because if they had chosen one the other privacy settings, less mis-matches would have occurred. However, since they need to make a conscious decision at this point, they need to know what the effects their choice will have.

5.2.3.2 Shopping cart

All participants understood and explained the shopping cart correctly; two of them especially mentioned that it was a nice way to visualize this type of information.

5.2.3.3 Shipping

All participants explained the shipping options correctly;

Three of the participants chose “parcel to parcel station” delivery since *“the parcel will not fit in my mailbox”, “I live close to my post office” and “it is the least expensive option”*. The other two chose Hermes since *“I am an exchange student from Greece and Hermes is a god from Greece”* and DHL insured since *“I ordered a DVD-player and an insured delivery feels most secure”*.

It is interesting to see that the only delivery option that is complying with the “nearly anonymous” privacy setting, “parcel to parcel station”, is not chosen by any participant because of the information that they will be required to release. All participants choose delivery options according to price and convenience within their daily life, not according to their privacy online.

5.2.3.4 Payment

They all understood what the payment options. They chose different options depending on which was cheapest, most secure, their normal way to shop and the least complicated option. None of them knew what the “PaySafeCard” was, but four of them explained it as some kind of secure way to shop online.

Two of the participants chose payment via VISA and the other three chose to pay on delivery.

Once again, their choices were made according to cost and convenience. One participant chose to pay on delivery, since she did not trust online money transfers, she was also the only one who had managed to choose options for delivery and payment that was in compliance with the “nearly anonymous” privacy settings. The other participants had chosen “parcel to parcel station” and VISA (2), Hermes/DHL and “pay on delivery” (2).

5.2.3.5 Sum

None of the participants understand why the summary field only contains the tax information and not a summary of all the costs. This is supposed to contain the complete sum if implemented but it is not working in this mockup.

5.2.3.6 My Data

5.2.3.6.1 Text fields

Four of the participants started to directly fill in information for the “My Data” field without looking at the table or seeing that there was a mismatch. When they came to the Address 2 line, none of them understood what this was for, only the three of them that chose “parcel to parcel station delivery” must insert this field. The “valid until” line was also confusing the participants, since they were used to choose this type of information from two dropdown lists and did not know if they should write “*May 2011*” or “*05/11*”.

Three of the participants only filled in the lines where there were stars,*, shown. None of the participants thought about or noticed the yellow and grey colours for the input fields.

From this, one can draw the conclusion that the colouring of input fields does not help these participants to see which information is required. The stars help but these need to be shown in a clearer relation to the text fields, since most participants focus on the fields first. The users might also need a more visible explanation to notify that the star visualizes mandatory fields.

5.2.3.6.2 Checkboxes

Two participants asked about the exclamation marks and one of them thought that he should be extra careful with disclosing this information, the other participant explained the exclamation marks correctly after exploring the mockup. The last three participants did not mention the exclamation marks at all.

The four participants, who had a mismatch, tried to check the boxes where the exclamation marks were shown, but could not do so, since they were not selectable. This confused these participants and they did not correlate this to the privacy setting they made earlier.

Only one participant explained the table correctly at first sight, while it took a lot more effort for the others to see the connections between the table and the other parts of the interface. This participant was also the only one, who thought that the table was a clear and good way to show the information.

5.2.3.6.3 Mismatch

Four of the five participants felt that the table was confusing them and that they did not really know why there was a mismatch or why it disappeared after they did some changes. The participants, who understood the table after a while, did so after the test leader more or less forced them to think about the different labels and the information given in the mismatch text.

Only two of the participants chose to change their privacy setting while the others either had no conflicts to begin with (1 participant) or changed their delivery/shipping options. They mentioned that they did not want to change the privacy settings or the delivery/shipping options and found it annoying that they were forced to do so.

The options available after selecting the privacy settings are not related to the options the participants actually can choose. Since all participants chose the “nearly anonymous” privacy setting, the options they can choose in accordance to this option are “parcel to parcel station” delivery, “PaySafeCard”, “prepay bank transfer” and “pay on delivery”. By letting the participants choose options that are not in compliance with their privacy settings, they will rather choose delivery and payment they are familiar with. They do not consider that this may result in a violation against their privacy settings, because they 1) are allowed choose these options and 2) are more concerned about the convenience of their everyday life.

5.2.3.7 Data to transfer

All participants explained this section correctly and they all appreciated it very much.

Three of the participants especially state that this is *“my favourite part of the mockup, something others can use”, “it is nice to see that not all companies get the same information since they all do not need it”* and *“good view, I like this”*.

5.2.3.8 Step 2 – Summary

All participants gave the correct answers as they did for Step 1 for this section of the mockup. Two of them thought that what was being shown here might include too much information. They mention that the table could easily be taken away, since the information also was shown in the “data to transfer” section.

This result was expected, since Step 2 includes the same information as Step 1, and the problems they had there were discussed before they were able to continue.

5.2.3.9 Step 3 – Confirmation

All participants said that when they entered Step 3 the purchase was completed and that Step 3 is a confirmation for which data they have sent, somewhat like a receipt.

When asked if they would like to see all this information once again, three of the participants answered with yes. Their reasons for this was that *“it might be interesting and it is nothing that disturbs me”* and *“if something did disappear I would be very confused about what and why”*. The other two participants thought that it made no sense to show the table since the data was also presented in the “data to transfer” section and that the privacy settings might not be interesting to see at the receipt since they do not have anything to do with the receipt.

5.2.3.10 Things to keep

The participants were asked for which parts of the system to keep and their answers were as follows.

“The design is good since it use a simple colouring; there is nothing unnecessary there which distracts the participant. The shopping cart, shipping and payment fields are nicely designed and show the information clearly.”

“The ‘data to transfer’ section is something I never thought about earlier and it is something I would like to know. The colouring with green and red is good so that I know when thinks are all right and when they are not.”

“The option to be able to select which information to send, but this way of choosing is not intuitive at all.”

“The design is OK and it is good that it is simple, I believe that everyone could learn to use this system. It is nice that there are no distractions, the system only shows the information needed and nothing more.”

5.2.3.11 Things to change

The participants were asked for which parts of the system to change and their answers were as follows.

“I would like to have more explanations shown the first time I use the system, these should then be accessible while using the mockup if I later forget things. It would be more intuitive and look more secure if the VISA-logo and DHL-logo and such were used so that it looks as if they are responsible for these parts. There is no way for me to know which parts are pre-checked and which part are not and this is very confusing.”

“I have an idea that the privacy settings should be on a separate page where they are explained in more detail so that it is clearer what they are about and what will happen if he choose them. The total of all items should be shown; the table does not need to be shown in step 2 since the “Data to transfer” show the same things in a better way. In step 3 I would like to only see the information from the ‘Data to transfer’ and the items purchased, as a receipt and information to whom it’s been transferred.”

“The table is the most complicated part of the system and I believe there needs to be an explanation about how the table correlates to the privacy settings, the delivery options and the payment options.”

“I would like to have a help function which can explain things to me.”

“The problematic parts of the interface are that one has to move from the table up to the privacy settings and back down again to change the things. There is no real connection between these sections and since they inflict on each other as much as they do they need to be closer to one another. It takes some time and some tries to understand this kind of systems but that it is expected to be like that.”

5.3 Discussions and conclusions

The main test results can be summarised as follows:

- The participants had no difficulties with understanding the Shopping cart, shipping, delivery and data to transfer sections of the interface.
- The “My Data” section was the part of the mockup that the participants had most difficulties with:
 - The text fields were the first thing the participants focused on and they filled in the information directly. Their focus on inputting information can be connected either to that the information to fill in was given in the scenario setup, but most probably also because they were used to fill in this type of information when purchasing products online. From the different indications on what information is mandatory to fill in, the yellow text fields were not noticed by any participants, while the stars were noticed by three of them. The stars for marking mandatory input fields are something the participants are familiar with, while the yellow fields are new to them. The fields “Address 2” and “Credit Card Expiry Date” are difficult for the participants to understand. The second address field for the reason that the participants did not know what this is for, and the expiry field since the participants are used to fill this in via a drop-down list.

- The checkboxes were confusing the participants, since they cannot check them if they chose “Nearly anonymous” privacy settings. The connection, between what information can be inserted while after having chosen different privacy settings is not displayed in a good manner. Most options are selectable while others are not, which creates a “mismatch” and is not compliant with the privacy setting used.
- The labelling and connection of the checkbox table rows and columns is not clear enough for the participants to see that they can select what information to send to which participant for what purposes. In addition to this comes the complexity of the possibility to create mismatches as discussed above.
- The “data to transfer” section was very appreciated by the participants as it gave them information they had before not thought about being so important to visualize and since it contains information they would like to know.
- Both “Step 2: Summary” and “Step 3: Confirmation” are understood correctly by the participants, even though some find that showing the “My Data” table does not add any new information to the information shown.

The recommendations that can be made after this test are the following:

- “My Data” section needs to be redesigned or, at least in Steps 2 and 3, be taken away completely, as the “data to transfer” field already visualizes what information will be sent to whom and for what purposes.
- Participants should not be able to select the options that are not complying with their chosen privacy settings. If the participants start by choosing their privacy settings, only the options available which match with these settings should be shown and be selectable. All other options can be greyed out and be made unselectable. Also, the fields for entering information should only be those requested (mandatorily or optionally) for the selected shipping and payment options.

Chapter 6

Policy Management & Display Mockups – 4th Iteration cycle

6.1 Introduction

The "PrimeLife Checkout" mockups of the 3rd iteration cycle presented in the previous chapter may give the user the impression that her privacy preferences are chosen by her at the services side and are matched at the services side with its privacy policy. As previous tests [30] have shown, users have anyhow difficulties with differentiating what the user side and what the services sides of an identity management system are. However, in PrimeLife all personal data managed at the user side are fully under the user's control and are only disclosed to others if the user consents to it, and it is important to mediate this to the user. For this reason, we have decided to integrate the user preference management into the user's browser in the 4th mockup iteration cycle, which is presented in this chapter (see sections 6.3 and 6.4).

After the PrimeLife Policy Language (PPL) has recently been specified by Activity 5 (see PrimeLife H5.3.2 and chapter 2), and after more intensive discussions on policy user interfaces have taken place between Activities 5 and 4 since autumn 2009, another important objective of the 4th iteration cycle was to produce UI mockups that specifically address the HCI requirements derived from PPL, as presented in section 2.2. These user interface proposals shall later, after they have passed our usability tests, be implemented as UIs for the PPL engine. The 3rd iteration "PrimeLife Checkout" mockups (which were developed before PPL was fully specified) assume that also information about the items ordered and prices will be sent from the services side to the user side, which is however not possible with PPL (PPL was at least not designed for communicating such type of information)..

HCI functional requirement derived from PPL as well as legal requirements, which the 4th iteration mockups should particularly address, are the following:

- Displaying the services side's policy in a usable manner as a basis for obtaining the user's informed consent. For this, we will follow the Art. 29 Working Party's recommendation of displaying policies in multiple layers.
- Assisting the user in the process of credential selection for proving certified personal attributes or properties requested by the services sides.

- Clearly displaying policy mismatches in an informative but not too strongly alarming manner, so that users will make rational decision on how to proceed. In case of a mismatch, the option to overrule the user's preferences for the current transaction or for all future transactions shall be offered to the user.

Moreover, PPL has the following properties that need to be taken into consideration:

- Personal data attributes requested for certain purposes cannot be marked as optional. Opt-ins for the use of attributes for certain purposes (e.g., use of an email address for marketing purposes) has to be done at the services side before the PPL request for personal data is sent to the user. If the user opts in at a site, the data request from that site will include the attributes for the purposes that the user opted in.
- It is possible to specify that data will be also forwarded to a third party (down stream controller), but the identity of that third party cannot be specified. If however, a site requests data, which should only be used by a specific data controller and is therefore encrypted with a key of that data controller, and the site forwards the encrypted data directly to that data controller, then it is possible to specify the identity of that data controller in PPL (e.g., if a web shop requests payment data encrypted with the public key of a payment provider, then the identity of the payment provider can be specified, which will act as a data controller).

The first version of the 4th iteration of policy mockups will be presented in the remainder of this chapter. They describe work in progress, and have not been tested yet. Some successive modifications and improvements can therefore still be expected.

6.2 Selecting Active Settings

The preference editor, as described in chapter 7, allows the user to create different privacy settings (i.e., privacy preferences), which can be specified with a name and icon. Figure 24 shows a menu to select the privacy settings that should be the active ones. The menu contains three predefined privacy settings (which we have called “Nearly anonymous”, “Minimal Data” and “Requested Data”) together with the customised “My Shopping” privacy settings. The menu also offers the option of having no active privacy settings with the “None” alternative. The consequence of having no active privacy settings when visiting a website that is PPL aware still needs to be specified. The user could either be forced to select a privacy settings or no policy matching will take place. The “Open Editor” on the bottom of the menu provides an option to open the preference editor to modify or create new profiles of privacy settings.

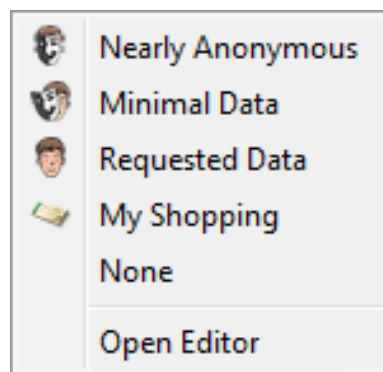


Figure 24. Selecting active privacy settings menu

6.3 Menu Placement

The menu shown in Figure 24 could be placed in two different places; as an extension to the bookmarks list or as part of the location bar.

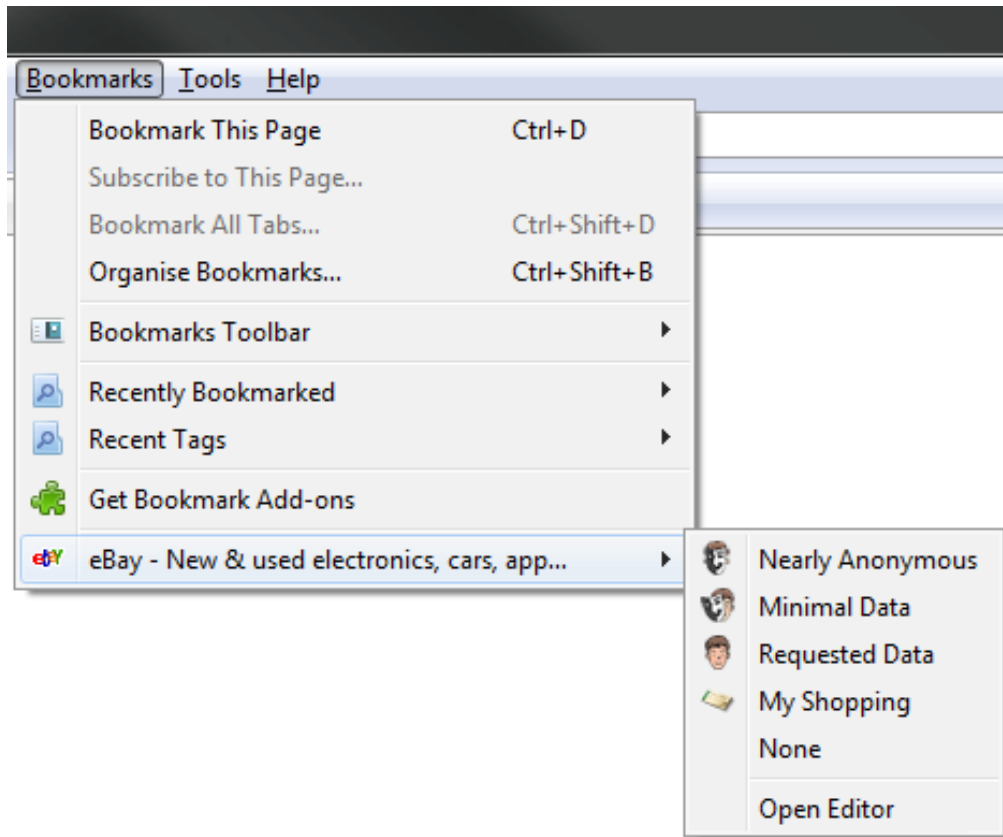


Figure 25. Bookmarks based approach

Figure 25 shows the menu as part of the bookmarks list (“Favorites” list in Explorer). This approach is an advanced version of the bookmarks based approach first proposed in PRIME Deliverable 6.1.b [29], in [29] and in [30], which however scales better than the one that was proposed in PRIME. It is analogous to how folders of bookmarks are displayed, where the bookmark is treated as a folder. Selecting privacy preference settings in the subfolder of a bookmark makes the browser go to the bookmark in question using the selected privacy settings as the active one.

In Figure 26, the icon for the user’s active privacy settings is shown in the location bar. By clicking the icon the menu in Figure 24 is shown, allowing the user to change to different settings. Note that the location bar approach allows the user to change privacy settings while already on a webpage; the bookmark based approach is limited to locations bookmarked by the user.

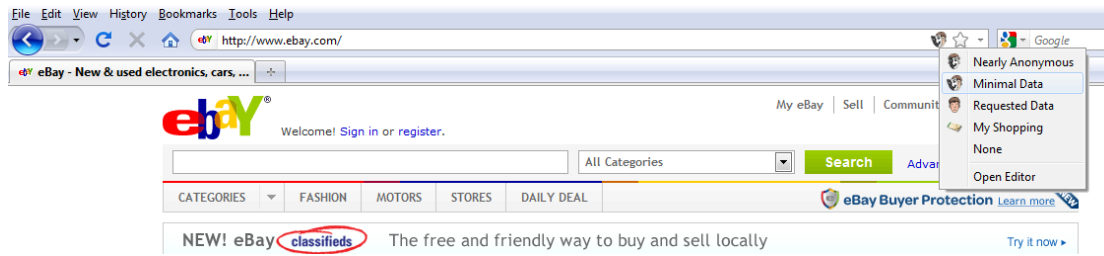


Figure 26. Location bar based approach

The bookmark and location bar approaches could be used in combination and be enabled by default with the option to disable either of them. Selecting privacy settings from the bookmarks menu would change the location of the browser and the active privacy settings. The icon would then be updated in the location bar to reflect the user's new choice. Any later change of the privacy settings in the location bar would override any selection made when browsing to the current site from the bookmarks menu.

6.4 Interface Authenticity

While the functionality shown in Figure 25, Figure 26 and Figure 27 would require a Firefox extension to be developed, since changes to Firefox needs to be made, there are several options for the “Send Data?” dialogue described in subsection 6.5. Java applets, using a regular web page with or without Flash or a Firefox extension among others are all viable alternatives (all requiring different approaches to communicate with the policy engine). Depending on which technology is used to implement the “Send Data?” dialogue, there is a need to prevent spoofing attacks where an attacker creates a seemingly identical interface and asks the user for information (commonly referred to as phishing) under the guise of being a genuine “Send Data?” dialogue.

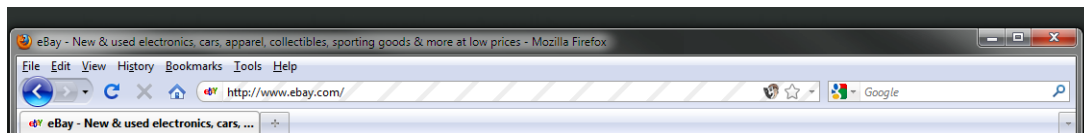


Figure 27. Striped location bar

Figure 27 shows one way to add authenticity to the interface by striping the background of the URL bar when the genuine “Send Data?” dialogue is shown to the user. Modifying the location bar can be accomplished by developing a Firefox extension. This is similar to how browsers modify the location bar when HTTPS is active, using different colors depending on the validity and type of certificate presented to the browser. Stripes have the advantage of being visible to color impaired users and usable together with the HTTPS colors (if they were to be used on the entire location bar as in previous versions of Firefox) by making the background of the stripes transparent.

6.5 The “Send Data?” Dialogue

In Figure 28, Figure 29, and Figure 30, the 4th iteration “Send Data?” dialogue mockups are displayed that pop up when personal data is requested by a communication partner.

In Figure 28, the background website is shaded grey, which is a usual HCI technique for putting the popup window more visibly into the foreground and thus into the user's focus.

As mentioned, we are following the Art.29 Working Party recommendation of displaying policy information in multiple layers. The “Send Data?” dialogue window is displaying the top layer and contains also a link to the full privacy policies of the data controllers.

The “Send Data?” interface, as depicted in Figure 29 and Figure 30, is structured into three sections: The section at the top of the side with the headline “Data requested by” provides information about the identities of the data controllers.

The middle section with the headline “Your data is requested for the following purposes” displaces what types of data are requested by the data controllers and for what purposes these data will be used. For presenting this, we use a two-dimensional table with data types as rows and purposes as columns, which closely corresponds to the simplified Grid of a Privacy Nutrition Label, as presented in [4]. As in [4], we also use an icon with a minus sign and a light-blue background colour for table entries to illustrate that no data of that respective data type is requested for the respective purpose. We also use an exclamation mark with a red background colour for informing the user that data is requested for a specific purpose and will be sent if the user presses the “send” button (see Figure 29). In an alternative mockup, we use instead a plus sign with red background colour (see Figure 30). As in our case, no data will actually be sent until the user presses “send”, an icon that is less alarming than the exclamation mark icon, may be more appropriate. How these icons will be perceived, needs to be analysed with our future usability tests.

In [4], further icons for data, for which the user needs to opt-in or opt-out, were used. In PPL however, it is not possible to specify opt-in or opt-out options for requested data items, and hence, we do not need icons for these cases in our user interfaces.

Further differences to the two-dimensional grid presentation in [4] are the following:

- In [4], an extra column with the headline “Who we share your information with” is included. By using an extra column, it is however not clear for what purposes the data will be passed on. In our UIs, we provide the information on whether data requested for a specific purpose will be transferred to a third party directly in the table entry with the help of the icon “-> ->”. In case that data is requested by different data controllers, the table entries also specify to whom data requested for a specific purpose will be sent with the help of the icon “->:” in front of the number of the data controller (as specified in the “Data requested by” section).
- Scroll-down boxes with freely changeable content are placed next to the data types allow the user to fill in or select data values that she would like to disclose for the requested data types. Values that she has filled in at the time of configuration or in previous transactions are filled for the ease of use. For data values for which a certification in form of a credential proof is requested, another box is used with the title “Certified By:”, with which the user can select the credential with which the proof will be made. The interface is also providing information on whether data requested for a specific purpose will be transferred to a third party (so-called “downstream data controller” in PPL).

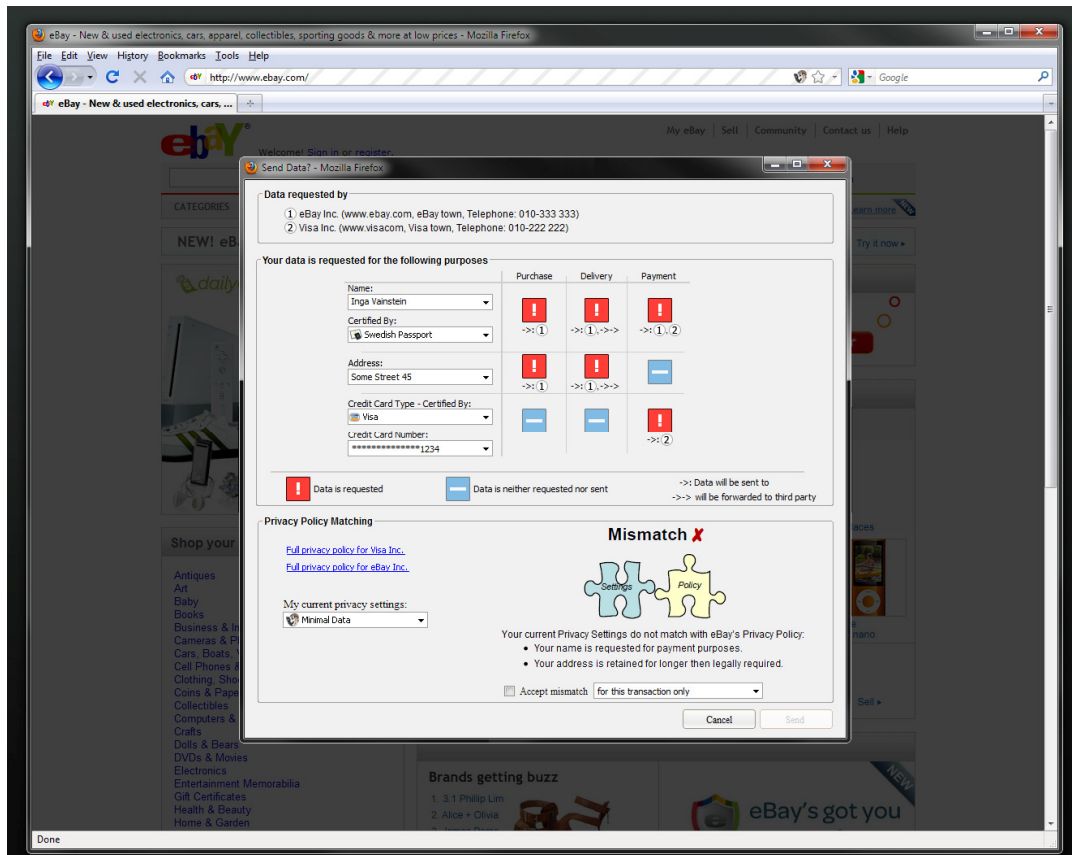


Figure 28. The user's screen showing the send data dialog, striped location bar and location based selection approach.

The lower section of the "Send Data?" Dialogue window with the headline "Privacy Policy Matching" displays how far the user's privacy settings are matching with the website's privacy policy. As in the "PrimeLife Checkout" mockups of the 3rd iteration cycle, we also use in this iteration cycle icons based on the metaphor of two puzzle pieces representing the user's settings and the site's policy, which are either fitting together (in case of a match) or not (in case of a mismatch, as depicted in Figure 29). The matching result is also given by the titles "Match ✓" (with ✓ in green colour) or "Mismatch ✗" (with ✗ in red colour) placed above the puzzles icon. The reasons for a mismatch are given in a bullet list below the puzzle icon.

The "Privacy Policy Matching" section also provides the possibility for the user to change her current privacy settings.

If there is a mismatch, unless the user wants to cancel the transaction, she can only proceed and send the requested data if she has checked the box marked with "Accept mismatch". By this, she explicitly accepts that her privacy settings are overruled. She has the options to either overrule her privacy settings only for the current transaction (which is the default), to accept the mismatch and update her current settings (this option is only offered if her current settings is not one of the predefined ones), or to accept the mismatch and update her privacy settings and save them as new settings under a new name. The last two options provide the user with the possibility to configure and fine-tune her privacy settings "on the fly".

Send Data? - Mozilla Firefox

Data requested by

- 1 eBay Inc. (www.ebay.com, eBay town, Telephone: 010-333 333)
- 2 Visa Inc. (www.visacom, Visa town, Telephone: 010-222 222)

Your data is requested for the following purposes

	Purchase	Delivery	Payment
Name: Inga Vainstein	!	!	!
Certified By: Swedish Passport	->: 1	->: 1, ->->	->: 1, 2
Address: Some Street 45	!	!	—
Credit Card Type - Certified By: Visa	—	—	!
Credit Card Number: *****1234			->: 2

! Data is requested
— Data is neither requested nor sent
->: Data will be sent to
->-> will be forwarded to third party

Privacy Policy Matching

Full privacy policy for Visa Inc.
Full privacy policy for eBay Inc.

My current privacy settings:
Minimal Data

Mismatch X

Settings
Policy

Your current Privacy Settings do not match with eBay's Privacy Policy:

- Your name is requested for payment purposes.
- Your address is retained for longer then legally required.

☐ Accept mismatch for this transaction only

Cancel
Send

Figure 29. The “Send Data?” dialogue with the “exclamation mark” icon for notifying users about data requests

Send Data? - Mozilla Firefox

Data requested by

- 1 eBay Inc. (www.ebay.com, eBay town, Telephone: 010-333 333)
- 2 Visa Inc. (www.visacom, Visa town, Telephone: 010-222 222)

Your data is requested for the following purposes

	Purchase	Delivery	Payment
Name: Inga Vainstein	+	+	+
Certified By: Swedish Passport	->: 1	->: 1, ->->	->: 1, 2
Address: Some Street 45	+	+	-
Credit Card Type - Certified By: Visa	-	-	+
Credit Card Number: *****1234			->: 2

+ Data is requested
- Data is neither requested nor sent
->: Data will be sent to
->-> will be forwarded to third party

Privacy Policy Matching

[Full privacy policy for Visa Inc.](#)
[Full privacy policy for eBay Inc.](#)

My current privacy settings:
Minimal Data

Mismatch X

Settings
Policy

Your current Privacy Settings do not match with eBay's Privacy Policy:

- Your name is requested for payment purposes.
- Your address is retained for longer then legally required.

☐ Accept mismatch for this transaction only

Cancel
Send

Figure 30. Alternative “Send Data?” dialogue with the “plus” icon for notifying users about data requests

Chapter 7

Privacy Preferences Editor

This chapter describes the design of the first version of the privacy preferences editor and the underlying motivations behind it. First a brief description of the tasks of the editor is given, followed by a detailed description of the design. The chapter ends with some relevant technical details of the implementation of the editor.

7.1 The Main Tasks of the Editor

The preference editor allows the user to specify, on an attribute level, what the conditions under which they which they would accept to disclose the data to a data controller. This is done by creating data handling preferences, which are matched against the privacy policies of the resources/websites that the user wishes to access. An example of a resource would be the checkout of an online store, where the user is required to disclose their home address, email and credit card information. The store needs to use the credit card information for billing purposes, the home address for delivery by DHL and the email address for marketing purposes. This information is contained in the store's policy.

7.2 The User Interface Design

Figure 31 shows a screenshot of the editor user interface. On the left side, the user's profiles of privacy settings are shown in a tree view. Each leaf in the view is an attribute type. The attributes are grouped in categories, which in turn are grouped into profile of privacy settings. When the user selects an attribute in the tree view, its data handling preferences are shown in the right part of the editor. If a category is selected, like in Figure 32, the user can set preferences for all the attributes that are part of the category. The checkboxes next to each category and attribute can be used to toggle if the attribute or category should be active or inactive.

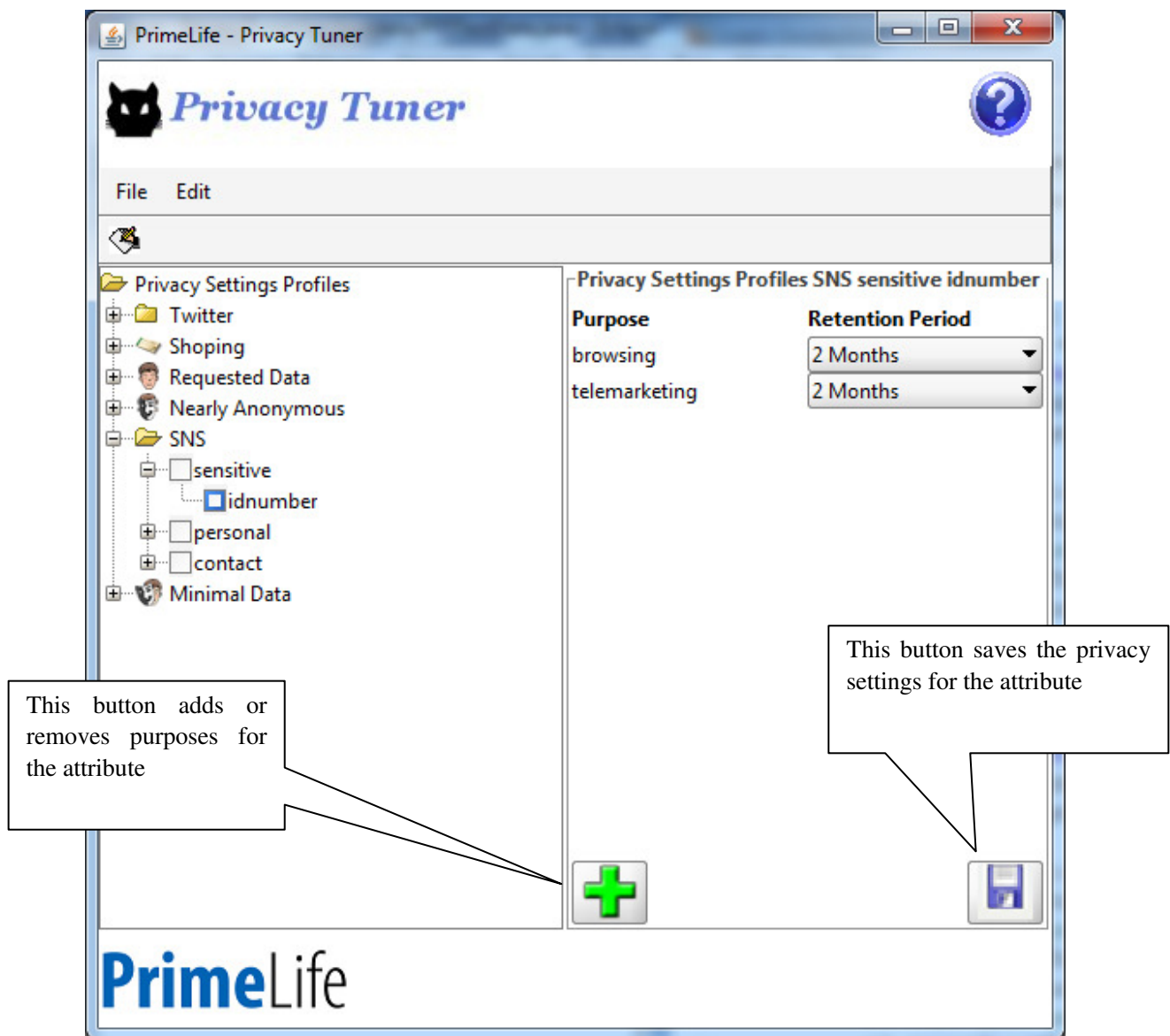


Figure 31. An overview of the editor's user interface, where preferences can be set for the selected attribute

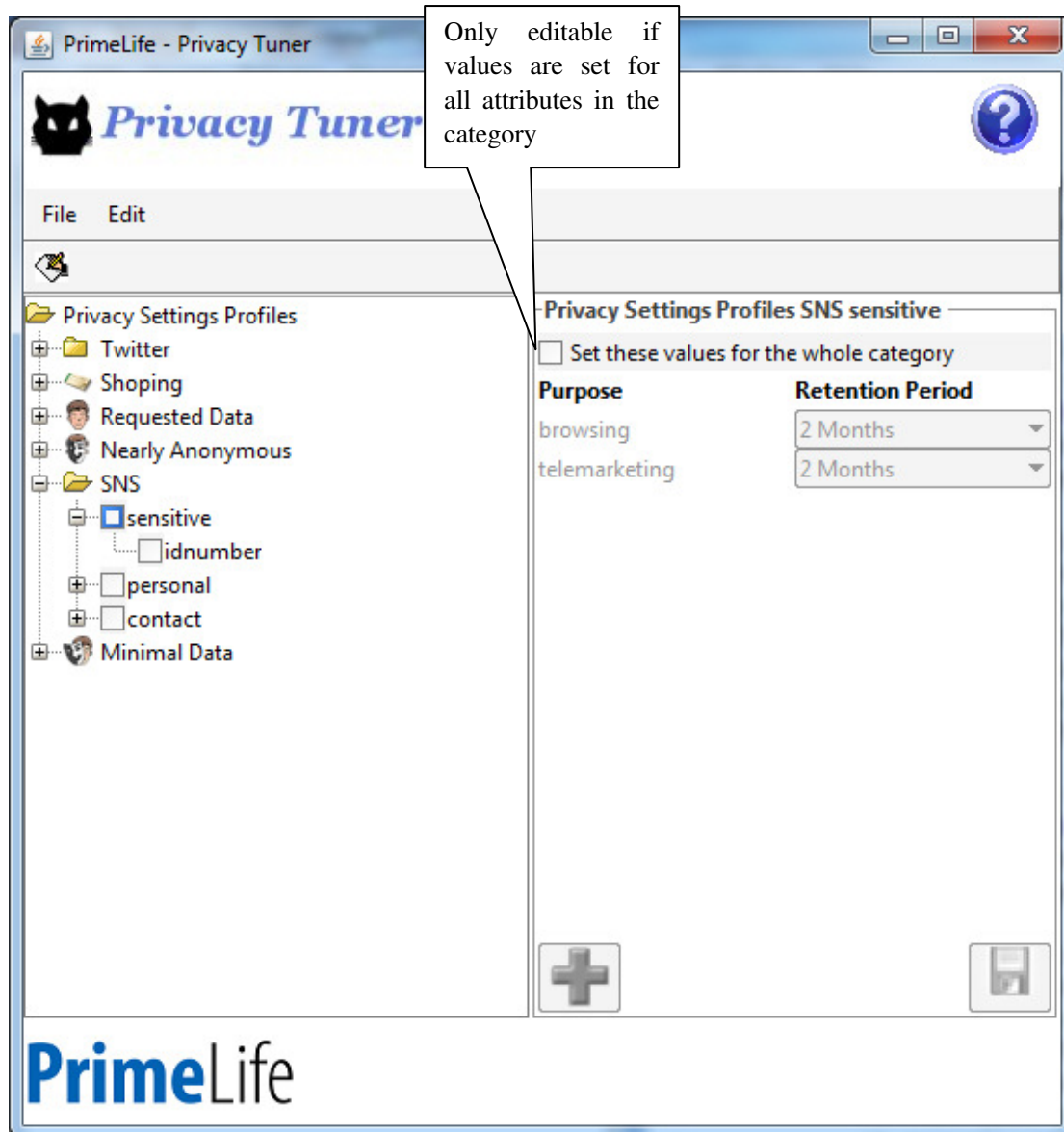


Figure 32. An overview of the editor's user interface, where preferences can be set for categories of attributes

The users can create their own profiles of privacy settings, for example for shopping and social networking sites, and specify their own preferences for the attributes they include into the profiles. We envision that the editor comes with predefined profiles, created by trusted parties. The editor should also allow the user to import and export profiles, to facilitate easy sharing of profiles between users and organizations.

7.3 Design Rational and Future Work

We opted for an attribute centric approach for the editor, because it is more concrete than specifying preferences on abstract data. To make the link between preferences and what they apply to stronger future versions of the editor could allow users to bind the preferences set on attribute types to specific attribute values. This would allow the user to create a profile that can be

used in conjunction with the other UI components to disclose, for example, a specific email address the user has, one used for work and another for personal activities.

Unfortunately the attribute centric approach makes the process of creating a new profile of privacy settings for several attributes quite time consuming. Therefore, the editor offers the ability to set preferences for categories of attributes. These categories currently have no relation to anything in PPL or any ontology specifying attribute types, but are created at the discretion of the user. Specifying a number of default sets of attributes grouped into standardized categories for the reason of consistency is a potential area of future work. Creation of profiles can be made easier by allowing them to evolve over time, based upon the decisions the user makes in other parts of the UI. This is supported by our privacy preference management “on the fly” approach (see above).

While the basic design of the editor is done, further work is needed to add functionality (like importing profiles) and to include more configurable preferences. The editor currently supports a small subset of the functionality offered by the PrimeLife Policy Language PPL, see chapter 2. Finding a balance between functionality and ease of use is of the utmost importance as the work continues.

7.4 Relevant Technical Details

The preference editor is implemented in Java where the GUI uses the Swing toolkit. HSQLDB is used as the database. The editor can be divided into three parts: the GUI, the database and the transformer. The GUI only works with the internal database and not directly on the policy store as part of the user’s policy engine. The main reason for this is because the API, provided by the policy engine, specifying on how the editor should manipulate the engine’s policy store is at the time of writing this not finished yet.

To ensure that we will be able to transform the user’s preferences into PPL and vice versa, to be able to import PPL preferences into the editor, we developed a number of small classes that parsed and generated PPL preferences. We refer to these classes as the transformer. To represent PPL preferences in Java we opted for the approach of developing classes that represents the different actions and triggers that makes up obligations in PPL. Purposes, as part of authorizations, are hardcoded URIs. As soon as the API for accessing the engine’s policy store is available the transformer will be updated to work against the API and made coherent.

Chapter 8

Conclusions

This deliverable has addressed the two major challenges of how to make privacy policies more comprehensible and transparent to end users and how to simplify the process of privacy preference management for them. For this, user interfaces must be developed that are informative, comprehensible while legally compliant, but also flexible to handle both simple and complex interactions involving data disclosures to several data controllers or for several purposes and possibly different retention periods.

In this deliverable, we have presented the HCI research and development work done within PrimeLife work package 4.3 during the last year to address these challenges. This work is a continuation of our work during the first sixteen months of the PrimeLife project, for which we have reported our first results in the Deliverable D4.3.1 on the first version UI prototypes for policy administration and presentation.

The last year's research and development work on UI prototypes for policy administration and presentation and the results achieved reported in this deliverable include our work and contributions in the area of privacy icons. Besides, it comprises the second to the fourth iteration cycles of policy management and display mockups developments by work package 4.3, from which iteration 2 and 3 have been tested with small groups of test users: The second iteration is based on multiple steps for displaying and managing policies, the third one is the so-called PrimeLife Checkout mockup and the fourth iteration we have developed a browser-integrated approach, which specifically aims at meeting HCI requirements derived from PPL. Furthermore, the implementation of a preferences editor was part of last year's work and is described in this Deliverable.

The work described in this deliverable is still work in progress. In particular, larger guided usability tests of the fourth iteration with 16 test persons are planned for this summer and are needed to decide on how to finally approach the following questions in the final interfaces to be implemented:

- *What is the best way to present important policy aspects to the users?* Our ongoing tests of policy icons should partly provide some further answers this question. Besides that, we still intend to investigate further what will be the best form for displaying what data is requested for which purposes. Related work reports good experiences with 2-dimensional grids [4] for summarising policies. Whereas tests of our multi steps mockups also showed that users appreciated a 2-dimensional table summary in step 6 showing what data will be

sent for what purposes, test users had more difficulties to understand the table summary in the PrimeLife Checkout mockup. The reason for this can however be the complex checkboxes and field colour codes used in that table that were not intuitive for the test users. Our planned usability tests the two versions of the fourth iteration of mockups, where data to be disclosed and purposes are presented either in a simpler 2-dimensional table as illustrated in chapter 6 or in a traditional form, will allow us to compare these two presentation approaches and to investigate this question further.

- *How to present policy mismatches?* Well-understandable presentation of policy matching results and reasons have been an issue, especially in the first two iteration cycles. The fourth mockup iteration presents this information prominently with a more detailed description and the use of illustrative icons. Our usability tests will show whether users will be well informed about the policy matching outcome and what it applies.
- *How to help users to configure their privacy preferences “on the fly” in a well understandable manner?* The usability tests of the second mockup iteration have revealed that users did not understand privacy preference management “on the fly” idea and tended to save changes to their preferences too quickly without understanding the implications. In the third mockup iteration, we provide a longer textual description for the different options that the user has (namely to accept a mismatch for the current transaction only, to accept the mismatch and update her current settings, or to accept the mismatch, update the privacy settings and save them as new settings). Again, our planned usability tests should reveal whether this makes the policy management “on the fly” approach better understandable.

The results of our usability will further guide the implementation of the user interfaces for the PPL engine. They will be reported in the final HCI research report at the end of the PrimeLife project.

References

- [1] J. Gross, J. Sheffield, A. Anderson, N. Yu, “Engendering Trust: Privacy Policies and Signatures”, Poster Proceedings of the Symposium of Usable Privacy and Security (SOUPS), July 14-16, 2006, Pittsburgh, PA, USA.
- [2] A. Herzog, “Usable Security Policies in Runtime Environments”, Linköping Studies in Science and Technology, Dissertation No. 1075. Linköping University, 2007, Sweden.
- [3] Article 29 Data Protection Working Party. Opinion on More Harmonised Information provisions. 11987/04/EN WP 100, November 25 2004, available online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.
- [4] P. Kelly, J. Bresee, L. Cranor, R. Reeder, “A ‘Nutrition Label’ for Privacy”, Symposium On Usable privacy (SOUPS) 2009, July 15-17, 2009, Mountain View, CA, USA.
- [5] M. Rundle, “International Data Protection and Digital Identity Management Tools”, presentation at IGF 2006, Privacy Workshop I, Athens, 2006, available online: <http://identityproject.lse.ac.uk/marty.pdf> (iconset cf. slide 8).
- [6] M. Mehltau, Iconset for Data-Privacy Declarations v0.1, 2007, available online: <http://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf>.
- [7] C.-M. Karat, J. Karat, C. Brodie, J. Feng, “Privacy in Information Technology: Designing to enable privacy policy management in organizations”, International Journal Human-Computer Studies 63 (2005), pp. 153-174.
- [8] C.-M. Karat, J. Karat, C. Brodie, J. Feng, “Evaluating Interfaces for Privacy Policy Rule Authoring”, in Proceedings of the SIGCHI conference on Human Factors in computing systems CHI 2006, April 22-27, 2006, Montreal, Canada.
- [9] C. Brodie, C.-M. Karat, J. Karat, “An empirical study on natural language parsing of privacy policy rules using the SPARCLE policy workbench”, Proceedings of SOUPS 2006, pp.8-19.
- [10] L.F. Cranor, P. Guduru, and M. Arjula, “User Interfaces for Privacy Agents”, in ACM Transactions on Computer-Human Interaction 13(2), June 2006.
- [11] J. Gideon, S. Egelman, L. Cranor, A. Aquisti, “Power Strips, Propylactis, and Privacy, Oh My!”, Proceedings of the Symposium of Usable Privacy and Security (SOUPS 2006), July 14-16, 2006, Pittsburgh, PA , ACM Digital Library.
- [12] J. Tsai, S. Egelman, R. Shipman, K. Pu, L. Cranor, “Symbols of Privacy”, Poster Proceedings of the Symposium of Usable Privacy and Security (SOUPS 2006), July 14-16, 2006, Pittsburgh, PA .
- [13] J.S. Pettersson, S. Fischer-Hübner, S. Pearson, M. Casassa Mont, “How Ordinary Internet Users can Have a Chance to Influence Privacy Policies”, Short paper Proceedings of the 4th Nordic Conference on Human-Computer Interaction - NordiCHI 2006, 14 - 18 October 2006, Oslo, Norway, ACM Press.
- [14] OASIS, “eXtensible Access Control Markup Language (XACML) Version 3.0”, 2009.
- [15] C. A. Ardagna, J. Camenisch, M. Kohlweiss, R. Leenes, G. Neven, B. Priem, P. Samarati, D. Sommer, M. Verdicchio, “Exploiting cryptography for privacy-enhanced access control”, Journal of Computer Security, vol. 18, no. 1, 2010.

- [16]C. A. Ardagna, S. De Capitani di Vimercati, S. Paraboschi, E. Pedrini, P. Samarati, M. Verdicchio, “Expressive and deployable access control in open web service applications”, IEEE Transaction on Services Computing, 2010, to appear.
- [17]J. Camenisch, S. Moedersheim, G. Neven, F.-S. Preiss, D. Sommer, “A card requirements language enabling privacy-preserving access control”, in ACM SACMAT 2010, to appear.
- [18]C. A. Ardagna, S. De Capitani di Vimercati, G. Neveny, S. Paraboschi, F.-S. Preiss, P. Samarati, M. Verdicchio, “Enabling Privacy-Preserving Credential-Based Access Control with XACML and SAML”, in IEEE Symposium on Trust, Security, and Privacy for Emerging Applications 2010, to appear.
- [19]D. Chaum, “Security without identification: Transaction systems to make big brother obsolete”, Communications of the ACM, vol. 28, no. 10, 1985.
- [20]S. Brands, “Rethinking public key infrastructure and digital certificates — building in privacy”, Ph.D. dissertation, Eindhoven, Institute of Technology, The Netherlands, 1999.
- [21]J. Camenisch and A. Lysyanskaya, “An efficient system for non-transferable anonymous credentials with optional anonymity revocation”, in EUROCRYPT 2001, ser. LNCS, vol. 2045. Springer, 2001.
- [22]D. Raggett, “H5.3.2 Draft 2nd Design for Policy Languages and Protocols”, PrimeLife Deliverable H5.3.2, 2009, available online: <http://www.primelife.eu/images/stories/h5.3.2-seconddesign/h5.3.2.html>.
- [23]L. Bussard, G. Neven, F.-S. Preiss, “Downstream usage control,” to appear at IEEE POLICY 2010.
- [24] S. Fischer-Hübner, E. Wästlund, H. Zwingelberg, “D4.3.1 UI prototypes: Policy administration and presentation version 1”, PrimeLife Deliverable D4.3.1, 2009 available online: <http://www.primelife.eu/images/stories/deliverables/>.
- [25]S. Fischer-Hübner, C. Köffel, E. Wästlund, P. Wolkerstorfer, “D4.1.1 HCI Research Report - Version 1“, PrimeLife Deliverable D4.1.1, 2009 available online: <http://www.primelife.eu/images/stories/deliverables/>.
- [26]E. Ehmann, M. Helfrich, “EG Datenschutzrichtlinie: Kurzkomentar“, 1999, Cologne, Germany.
- [27]W. Däubler, T. Klebe, P. Wedde, T. Weichert, “Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG”, Frankfurt, 2009.
- [28]Nielsen, J., Why You Only Need to Test with 5 Users, 2000, available online: www.useit.com/alertbox/20000319.html.
- [29]J.S. Pettersson, “HCI guidance and proposals”, PRIME deliverable, D6.1.c, 11 February 2005, available online: https://www.prime-project.eu/prime_products/reports/arch/.
- [30]J.S. Pettersson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, T. Kriegelstein, S. Clauss, H. Krasemann, "Making PRIME Usable", Proceedings of the Symposium of Usable Privacy and Security (SOUPS), 4-6. June 2005, Carnegie Mellon University, ACM Digital Library.

Appendix A

Pre-test Questionnaire & Test Scenarios for the Policy Display and Management Mockups (2nd iteration) Tests

A.1 Appendix 1: Pre-test information and Task

A.1.1 Introduction

The PrimeLife project develops user interfaces that make privacy policies more transparent to the end users.

A privacy policy of a services side specifies what personal data is requested from the user, the contact details of the services side requesting these data and for what purposes the data shall be processed.

A user can in turn define so-called **privacy preferences** (or short: *PrivPrefs*), which specifies which data categories or data values he/she is willing to release to a services side for what purposes.

If, during a transaction, a services side's privacy policies requests more data or wants to use data for other purposes than allowed by the user's preferences, the user should be informed about this mismatch. This helps users to spot parts of privacy policies they don't agree with, in contrast to traditional approaches where users have to read and understand long legal clauses within privacy notices.

In PrimeLife, we have defined one default privacy preference, which the user can choose, called "Minimal Data". It expresses the user's preference to release for a specific application (e.g. for E-Shopping) only the minimal amount of data for the purposes that need to be pursued for that application (e.g. payment and delivery for E-Shopping).

A.1.2 Your task

You have just installed your PrimeLife-system. During that installation you have entered some personal data into the system. This is only needed the first time you use the PrimeLife system. (Of course you are able to change these data later if you like).

In this case, we have already installed the system and entered fictions data for you.

Imagine that you have found a website called “YourSHOP”. This site was recommended to you by a friend you trust. He has ordered books from here for years and always gets coupons sent to him with great offers as a part of their marketing. Now you are looking for a special book and want to try “YourSHOP” and later receive their coupons.

Order the book “Guineas World Records 2010”. Think aloud and try to explain to me what the result means to you.

A.2 Appendix 2: Pre-test questionnaire

1. Your sex:

- ☐ Male
- ☐ Female

2. Your age: _____

3. How often do you use Internet?

- ☐ Once or several times a day
- ☐ Once or several times a week
- ☐ Once or several times a month
- ☐ Once or several times a year
- ☐ Never

4. How often do you shop on the Internet?

- ☐ Once or several times a day
- ☐ Once or several times a week
- ☐ Once or several times a month
- ☐ Once or several times a year
- ☐ Never

A.3 Appendix 3: Agreement

With this I give my permission to use the result, from the usability test session that I have participated, in the PrimeLife-project.

The purpose of this test is to evaluate a prototype from the PrimeLife project.

The test leader assures that all information received from this test session is treated confidentially.

I am aware that I can end the test session whenever I want to.

Date for the agreement and performance of the test

Signature of the test subject

Signature of the test leader
Maria Lindström

Clarification of the signature

Appendix *B*

Pre-test Questionnaire & Test Scenarios for the Policy Display and Management Mockups (3rd iteration) Tests

B.1 Test Scenarios

B.1.1 Usability Tests

The test is anonymous, you will be given a randomly chosen number and it is only through this number your answers can be identified.

If you want to abort the test at any time you are free to do so.

If there are any questions you feel that you cannot complete this is the best answer for showing that there is something really bad about the design. The software is supposed to be used by everyone in the society and not only computer experts. It is the software that is being tested and not you, so if there is something you do not understand we have basically designed it wrong.

The test leader will ask you questions during the test and take notes.

Some parts of the software are not implemented since it is a prototype. The software is also thought to be used as a separate software and not implemented in a web browser as it is today.

On the screen in front of you the software which is to be tested is shown. Read the instructions below and we will then have a discussion concerning the software.

B.1.2 Background to the test of today

You have just installed a new software, "PrimeLife", which is used to protect sensitive information about you when shopping online. You have put some products in your shopping cart at the web shop "Webshop", and to complete your purchase you have chosen to use "PrimeLife". The window shown on the computer screen then pop up.

Your name is Anders Anderssson and you live on Väg-gatan 42, 123 54 Stadsala in Sweden. You have e-mail address anders@anderssson.se, phone number 012-345678, credit card number 1234 1234 1234 1234 with verification code (CVV) 123 and it will expire in May 2011. Your closest postal office is at Väggatan 43.

How would you proceed to complete your purchase?

B.2 Pre-test Questionnaire (translated from Swedish)

1. Gender:

☐ Man

☐ Woman

2. Age: _____

3. How often do you use internet?

☐ Once or several times a day?

☐ Once or several times a week?

☐ Once or several times a month?

☐ Once or several times a year?

☐ Never?

4. How often do you shop on the internet?

☐ Once or several times a day?

☐ Once or several times a week?

☐ Once or several times a month?

☐ Once or several times a year?

☐ Never?

5. What type of services do you usually use online?
