

# Final HCI Research Report

Editors:	Cornelia Graf, (CURE)
	Christina Hochleitner, (CURE)
	Peter Wolkerstorfer, (CURE)
	Julio Angulo, (KAU)
	Simone Fischer-Hübner, (KAU)
	Erik Wästlund, (KAU)
Reviewers:	Benjamin Kellermann, (TUD)
	Ronald Leenes, (TILT)
Identifier:	D4.1.5
Type:	Deliverable
Class:	Public
Date:	May 20, 2011

## Abstract

This deliverable provides an overview of recent research results of Activity 4 ‘Usability’ of PrimeLife, where an emphasis is put on those results, which have not been reported in the same detail in other HCI-related PrimeLife deliverables yet.

The first part reports about our results in the area of User Interface (UI) Representation of Privacy-enhancing Identity Management Concepts and presents research on PET methodologies, mental models for anonymous credentials and the results from the final round of end-user evaluations of the UI prototypes developed during the PrimeLife project. The second part reports about our work in the area of usable privacy policies and presents the final results of Activity 4’s research on policy icons and on a user-friendly management and display of PPL (PrimeLife Policy Language) policies.

# 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 2011 by KAU, CUR, ULDE.

# 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	Simone Fischer-Hübner (KAU)
Introduction	Simone Fischer-Hübner (KAU)
Research Results – UI Representation of Privacy- enhancing Identity Management Concepts	Julio Angulo (KAU) – Section 2.3.6 and editorial work Simone Fischer-Hübner (KAU) – Editorial work Cornelia Graf (CURE) – Section 2.3 Christina Hochleitner (CURE) – Section 2.3 Peter Wolkerstorfer (CURE) – Section 2.3 Erik Wästlund (KAU) – Sections 2.1 and 2.2
Research Results – User Interfaces for Policy Display and Administration	Julio Angulo (KAU) – Section 3.2 Simone Fischer-Hübner (KAU) – Section 3.2 and editorial work Conny Graf (CURE) – Input for Section 3.2 Marit Hansen (ULD) – Section 3.1 Leif-Erik Holtz (ULD) – Section 3.1
Conclusion	Simone Fischer-Hübner (KAU)



# Executive Summary

The PrimeLife Activity 4 on “Usability” has had the objective to research and develop User Interfaces (UIs) for PrimeLife technologies, which are intelligible, user-friendly while compliant with legal privacy principles, and which are mediating trust.

This final HCI Research report presents recent results of PrimeLife Activity 4, where a focus is put on those results, which have not been reported in detail before in other PrimeLife project deliverables.

In the second Chapter, we present results by Work Package 4.1 on “UI Representation of Privacy-enhancing Identity Management Concepts. First, we present PET-USES (“Privacy-Enhancing Technology Users’ Self-Estimation Scale”), which is a questionnaire that we developed in PrimeLife for evaluating both the general usability of the system and additional PET-related aspects. PET-USES can therefore add valuable knowledge to PET UI developers and has thus been used by Activity 4 for the post test interviews that we did for the PrimeLife prototype usability evaluations.

Moreover, we summarise results of research that we conducted in regard to the user’s mental models of anonymous credentials, which reveal that the selective disclosure property of anonymous credentials is difficult to show. It demonstrates that inducing adequate mental models is a key challenge that needs to be addressed for making novel privacy technologies well usable.

Furthermore, we present a summary of our results of the final PrimeLife prototype evaluation conducted at CURE and Karlstad University. Evaluated prototypes were: Clique, Dudle, Reputation Management Wiki and the Privacy Dashboard. The usability evaluation showed that in general the evaluated prototypes were accepted well by the test users, who were able to handle the current versions of the prototypes. However, some changes and adoptions would improve the usability and workflow of all prototypes. Besides, results of an expert evaluation of the Scramble! prototype, which was done at Karlstad University, is presented including a list of recommended UI improvements for making it more attractive also for non-expert users.

The third Chapter presents the final results of WP4.3 on “User Interfaces for Policy Display and Administration”. In particular, we present and motivate the final privacy policy icon set developed by ULD, which was elicited based on the icon tests that were conducted at Karlstad University and CURE. Besides, the work on “Privicons” by researchers at Stanford University, PrimeLife and other researchers is presented, which are dedicated icons that senders can attach to their emails to express their privacy preferences for handling this email. The need for standardisation of privacy icons is emphasised. We also present the test results of the 6<sup>th</sup> iteration cycle for the “Send data?” dialog UI for policy management and display and the UI of the improved 7<sup>th</sup> iteration cycle, which was implemented for the PPL (PrimeLife Policy Language) engine. Those final improvements that we implemented included tool tips, adding meaningful but simple icons to the credentials, help text via the context help icons, as well as dimming the possibility to accept mismatches if there is no mismatch.

The final (fourth) Chapter concludes with summarising main results and final remarks.



# Contents

<b>1.</b>	<b>Introduction</b>	<b>13</b>
1.1	Background .....	13
1.2	Deliverable Scope and Relation to other HCI-related PrimeLife Deliverables ...	13
1.3	Structure of this Deliverable .....	14
<b>2.</b>	<b>Research Results – UI Representation of Privacy-enhancing Identity Management Concepts</b>	<b>15</b>
2.1	PET-USES .....	15
2.2	Mental Model Research .....	17
2.2.1	Introduction.....	17
2.2.2	The users’ mental models of anonymous credentials .....	17
2.3	Research Results from the PrimeLife Prototype Evaluation .....	21
2.3.1	Demographic Data .....	22
2.3.2	Clique.....	22
2.3.3	Dudle.....	30
2.3.4	Reputation Management Wiki .....	37
2.3.5	Privacy Dashboard.....	39
2.3.6	Scramble!.....	43
2.3.7	Conclusions.....	49
<b>3.</b>	<b>Research Results – User Interfaces for Policy Display and Administration</b>	<b>50</b>
3.1	Policy Icons.....	50
3.1.1	Introduction.....	50
3.1.2	Related work .....	51
3.1.3	The early PrimeLife icon sets .....	51
3.1.4	Test results .....	52
3.1.5	Requirements for widespread usage .....	54
3.1.6	The PrimeLife icon approach .....	55
3.1.7	Excursus: Privicons.....	59
3.1.8	Conclusion and outlook .....	60
3.2	Policy Management and Display – 7 <sup>th</sup> Iteration cycle .....	61
<b>4.</b>	<b>Conclusions</b>	<b>65</b>
	<b>References</b>	<b>67</b>
	<b>Appendix A: PET-USES</b>	<b>70</b>
	<b>Appendix B: Usability Heuristics</b>	<b>72</b>





# List of Figures

Figure 1: Credential Selection: Card-based approach for the first round of tests cutting out attributes to be revealed as part of a newly created virtual card. ....	18
Figure 2: Credential Selection: Card-based approach for the first round of tests blacking out non-disclosed attributes.....	18
Figure 3: Credential Selection: Attribute-based approach for the second round of tests. ....	19
Figure 4: Credential Selection: The adapted card-based approach for the third round of tests, which combines the ideas of the first two rounds. ....	19
Figure 5: Clique: Screenshot of Inga's User Profile (Image was cut at the grey-red line for displaying the parts of the UI with which the user has to interact.).....	23
Figure 6: Clique: Enabling a Face.....	24
Figure 7: Clique: Labelling of Contacts and Members .....	25
Figure 8: Clique: Invite Contacts Label .....	26
Figure 9: Clique: Add members after the collection wizard is finished.....	27
Figure 10: Clique: Publish Button.....	28
Figure 11: Clique: Drag and drop functionality .....	29
Figure 12: Dudle: Main Page .....	30
Figure 13: Dudle: New Account .....	32
Figure 14: Dudle: Create Button Position .....	33
Figure 15: Dudle: Columns vs. Options.....	34
Figure 16: Dudle: Feedback anonymous voting .....	35
Figure 17: Dudle: Invite Participants .....	36
Figure 18: Dudle: Clickable Link .....	37
Figure 19: Reputation Management Wiki: User Interface (Image was cut at the grey-red line for displaying the important parts in this deliverable) .....	38
Figure 20: Reputation Management Wiki: Heat map .....	39
Figure 21: Privacy Dashboard.....	40
Figure 22: Privacy Dashboard: Query results .....	41

Figure 23: Privacy Dashboard: Preferences .....	42
Figure 24: Privacy Dashboard: Check Site Buttons .....	43
Figure 25: Scamble!: No possibility to populate contacts automatically .....	44
Figure 26. Scamble!: Unintuitive Settings .....	45
Figure 27. Scamble!: Confusing interaction flow in the Crypto Dialog and Key Chain editor ....	47
Figure 28. Scamble!: Obscure search functionality .....	48
Figure 29: Excerpt of well-rated icons .....	52
Figure 30: Storage icon .....	53
Figure 31: Excerpt of low-rated icons for "Friends of friends" .....	53
Figure 32: Excerpt of low-rated icons for "Friends" .....	53
Figure 33: Excerpt of well-rated icons for the recipient groups "Selected individuals" and "Public" .....	53
Figure 34: Proposal for PrimeLife icons .....	56
Figure 35: Proposal for a commercial interest icon.....	58
Figure 36: Proposal for an icon stating that there will be no aggregation with profile data.....	58
Figure 37: Excerpt of icons for SNS usage .....	58
Figure 38: Privicons .....	60
Figure 39: “Send Data?” dialog: Design of the 6 <sup>th</sup> iteration cycle .....	62
Figure 40: “Send Data?” dialog: Design of the 7 <sup>th</sup> iteration cycle .....	64

## List of Tables

Table 1: Proportions (and count) of errors of omission, correct responses and errors of addition in the card based approach, the attribute based approach, and the adaptable card approach .....	20
Table 2: Number of evaluations per prototype.....	22



# Chapter *1*

---

## Introduction

---

### 1.1 Background

It is the vision of PrimeLife to bring sustainable and user-controlled Privacy and Identity Management to future networks and services such as collaborative workspaces or social networks. Especially in these areas, user-controlled Privacy and Identity Management implies that users can make informed decisions about the release of their personal data, the selection of credentials for proving these information as well as decisions involving privacy and trust policy settings.

In order to enable users to make informed decisions, user interfaces (UIs) that inform them about the privacy policies and the trustworthiness of their communication partners as well as the release of personal data, are needed.

The goal of these user interfaces is to be informative, intuitive, legally compliant and well understandable without being intrusive. Hence it is the goal of PrimeLife Activity 4 to support the design of such UIs and to evaluate if developed prototypes in PrimeLife are useable and understandable for end-users. In this Final HCI (Human Computer Interaction) Research report deliverable, we present results which were gained in Activity 4 during the PrimeLife project.

### 1.2 Deliverable Scope and Relation to other HCI-related PrimeLife Deliverables

A focus of this deliverable is on project results, which have not been reported in detail yet in other PrimeLife project deliverables, in order to avoid major overlaps. It is therefore differs in the following ways from the following HCI-related PrimeLife Deliverables:

The PrimeLife book (D3.2.1) is in its Part III (“Human Computer Interaction”) providing a summary of the most relevant research results of the PrimeLife HCI Activity, which were achieved in the first 32 project months. In this Final HCI Research Report, we are providing some more details for some of these research results. Furthermore, we are presenting final results which were achieved in the last 8 project months. These are mainly results by WP4.1 (“*UI Representation of Privacy-enhancing Identity Management Concepts*”) on HCI methodologies for PETs, mental model research and the usability evaluation of the PrimeLife prototypes, as well as recent research results of WP4.3 (“*User Interfaces for Policy Display and Administration*”) on

policy icons and UIs for policy display and management, which we achieved in the last half project year. Earlier results by WP4.3 were reported in D4.3.2 on “UI prototypes: Policy administration and presentation – Version 2” as well as in the PrimeLife book chapter on “HCI for Policy Display and Administration”. The final results of WP4.2 were already summarized in the PrimeLife book chapter on “Trust and Assurance HCI” and in the recent Deliverable D4.2.2 on “End User Transparency Tools” and are thus not presented in this deliverable once again.

The Deliverable D4.1.6 on “Towards Usable Privacy Enhancing Technologies –Lessons learnt from the PrimeLife project” reports about lessons learnt from the PrimeLife HCI Activity by discussing typical HCI challenges and fallacies for privacy-enhancing technologies (PETs) that we experienced during the PrimeLife project. It also provides guidance on how these issues can be addressed in order to develop usable privacy-enhancing technology solutions. According to the initial PrimeLife work plan, these findings and guidelines were supposed to be reported as part of this Final HCI Research Report. However in order to give these project results more emphasis we decided to rather publish them in an extra deliverable, which can more visibly serve as an experience report and guidelines for all HCI designers of PET user interfaces. Hence, this deliverable will only briefly summarise conclusions in regard to lessons learnt and practical conclusions drawn from our HCI work in WP4.1 and WP4.3.

## **1.3 Structure of this Deliverable**

The remainder of the deliverable is structured as follows:

The second Chapter presents the results of WP4.1. In this Chapter, we present developed PET methodology in PrimeLife project, the so called PET-USES. Afterwards we summarise result of research that we conducted in regard to the user’s mental models of anonymous credentials. Furthermore, we present a summary of our results of the final PrimeLife prototype evaluation conducted at CURE and KAU. Evaluated prototypes were: Clique, Dudle, Reputation Management Wiki, the Privacy Dashboard and the “Send Data?” dialog. Besides, we present the results of an expert usability evaluation of the Scramble! prototype. We also present design implications and suggestions for improvements except for the “Send Data?” dialog, for which we present the evaluation results in Section 3.2.

The third Chapter presents the final results of WP4.3. In particular, we present and motivate the final privacy policy icon set and present the results of the 7th iteration cycle for the UIs for policy management and display, which were implemented for the PPL (PrimeLife Policy Language) engine.

The final (fourth) Chapter provides main conclusions and final remarks.

# Chapter 2

---

## Research Results – UI Representation of Privacy-enhancing Identity Management Concepts

---

This Chapter presents recent research results of WP4.1 (“*UI Representation of Privacy-enhancing Identity Management Concepts*”). In the area HCI methodologies for PETs the most important instrument, which WP4.1 developed was a usability scale for PETs, presented in Section 2.1. Furthermore, WP4.1 conducted research on the user’s mental models and user comprehension of privacy-related issues and PET concepts, which will be described in Section 1.1. Furthermore, WP4.1’s task has been the usability evaluation of PrimeLife prototypes. Section 2.3 briefly summarises the results final evaluation round and recommendations given for usability improvements. More details about the usability evaluations and recommendations for design improvements can be found in the PrimeLife Heartbeat Deliverable H4.1.3 (“User Evaluation Report”).

### 2.1 PET-USES

Usability evaluations of PETs are, in many ways, not different from any other usability tests. However, in examining the usability of PETs it is important to also investigate the users’ understanding of the application and its usage. In a number of our user tests we have noticed that users might very well solve a given task satisfactory and subsequently say that they liked the application and would recommend it, but, when asked about the consequences of their actions it turns out that they have not understood the main point of using the application. The problem is that the current questionnaires for measuring user experience, usability and various HCI (human-computer interaction) aspects such as the hedonic quality [Has2003] of both, software and websites [Bro96, TS04] focus on the usability of the primary task of the system.

The PET-USES (Privacy-Enhancing Technology Users’ Self-Estimation Scale) [WWK09] is a questionnaire that enables users to evaluate PET user interfaces both in terms of the primary task and specific PET related secondary tasks. Thus, the PET usability scales have a dual purpose.

They evaluate the system's general usability and the extent to which the system assists the user in learning and understanding privacy related issues.

The PET-related aspects modules currently developed are: Data Management, Credential Management, Privacy Preferences, Recipient Evaluation, Data Release, and History. They can all be used to evaluate specific PET-related functionality of software or web sites. The complete PET-USES questionnaire is available in Appendix A.

The focuses of the scales are the following privacy-critic areas:

- Data-management: The extent to which the system makes it easier to store and organize personal information. This scale can be used to evaluate all types of identity management software and services.
- Credential-management: The extent to which the system makes it easier to store and organize certificates and credentials. This scale can be used to evaluate identity management systems that include issued claim credentials (e.g. the Higgins project<sup>1</sup>).
- Privacy Preferences: This scale is designed to measure the extent to which the system makes it easier to set general and excessive levels for data release policies and to what extent the user is informed of unwanted data dissemination. Thus, an aspect of this scale is the decision support qualities of the system.
- Recipient Evaluation: the extent to which the system helps users to evaluate the data recipients' credibility and trustworthiness. This scale can also be regarded in terms of decision support.
- Data Release: The extent to which the system clarifies what personal information is being released and who is the recipient of the data.
- History: The extent to which the system can show the user when, what and, to whom personal information has been released and thus provide an overview of what data any given service provider might have accumulated.

An important feature of the measurement of PET-aspects is the modularity of the questionnaire, enabling the inclusion or exclusion of scales measuring specific aspects based on the tasks and features being evaluated, e.g. dependent on the context of use, the Credential Management part could be excluded from the questionnaire.

Developing the PET-USES within the PrimeLife project has resulted in some noteworthy experiences. First of all, interest in the PET-USES from parties outside of PrimeLife shows that there is a gap in the current range of available usability tests. Secondly, using the PET-USES during short cycle iterations in combination with small sample tests is rather difficult as the effects most often are rather small. However, it is nevertheless possible to compare user's comprehension and ratings of different aspects of a system. In essence, the comparison is then made between the different PET-aspects of a system UI rather than between different implementations of the UIs. Thus by using the PET-USES it is possible to learn what parts of a GUI one should focus on in order to maximize user comprehension of a complex PET-system. This approach was, for example, used in the evaluation of the PRIME IPv.3 where the results showed that users understood the History aspects of the UI but that they had difficulties in comprehending the Privacy Preferences and Recipient Evaluation aspects [Pri10a].

In sum, the PET-USES is a usability test that lets users evaluate both the general usability of the system and additional PET-related aspects and thus adding valuable knowledge to PET UI developers.

---

<sup>1</sup> [www.eclipse.org/higgins/](http://www.eclipse.org/higgins/)



## 2.2 Mental Model Research

### 2.2.1 Introduction

A mental model is an individual's inner representation of how something works in the real world. As such, mental models guide users in novel situations. As mental models shape our behavior, including how we approach tasks, they can provide clues to the mental processes that give rise to specific actions. [Joh86, Jon95, You08].

Using a mental model can be very helpful as it can guide the direction of design and the solution being worked on [You08]. To understand the reasoning behind the user's behavior it is important to understand the decision model that users use. If technology is designed building on the assumption that users have a correct mental model on privacy, it will not induce the desired behavior when users are in fact making choices based on a different model. The outcome of a mental model investigation is a reflection of the users' conception and ideas on how things work in reality. This knowledge allows practitioners to design and develop tools which support users' mental models and help correcting their misconceived mental models.

In the PrimeLife project we conducted research to investigate the users' mental models of various privacy-related aspects. In the following Sections, we summarize our research of the users' mental models of anonymous credential technology, which is a key privacy technology for enforcing data minimisation for applications. Further details on the first two test rounds described in the Section below are also described in [WFH11]. The third test round has only been conducted recently and has not been described in previous PrimeLife Deliverables before.

### 2.2.2 The users' mental models of anonymous credentials

Data minimization is a fundamental privacy design principle which essence is that all applications and services should use only the minimal amount of data necessary for the transaction at hand. The objective is, of course, to preserve the privacy and minimize possibility to profile users based on their behavior. A key technology in achieving data minimization is anonymous credentials [Cha85, Bra99, CL01]. A traditional electronic credential is a set of personal attributes that is bound to an individual by cryptographic means and that the user can use to prove these attributes. All usage of such a credential entails showing all attributes in the set irrespective of the demands of the current transaction. In contrast, anonymous credentials allows the user to reveal any possible subset of attributes of the credential, prove possession of the credential without even revealing the credential itself, and offer the possibility of so-called greater-than proofs.. For example, a user with a governmentally issued anonymous drivers license credential, can, using zero knowledge proof, reveal and prove any one of the following; her birth date, her birth day, being over or under any given age, or the fact that she has a valid driver's license without revealing any other attributes of the credential.

In order to investigate the users' understanding of an anonymous credential selector interface we performed three rounds of tests based on different mental models of anonymous credentials. The first round of tests (Figure 1 and Figure 2) was based on the card metaphor i.e. users were asked to select the source cards of the credentials, whereas the second round of tests (Figure 3) was based on an attribute based approach where the users were asked to select specific verified attributes they possessed.

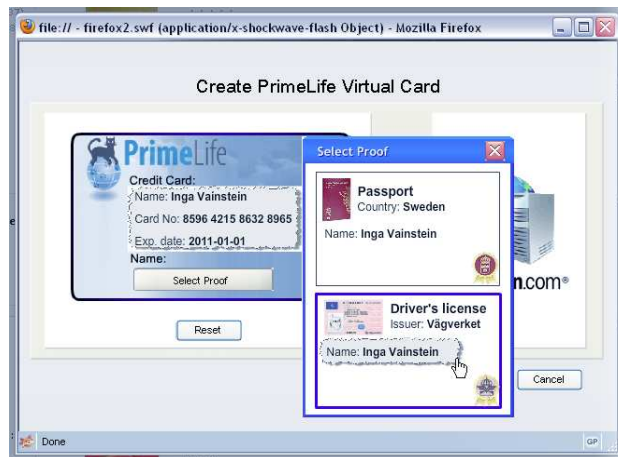


Figure 1: Credential Selection: Card-based approach for the first round of tests cutting out attributes to be revealed as part of a newly created virtual card.



Figure 2: Credential Selection: Card-based approach for the first round of tests blacking out non-disclosed attributes

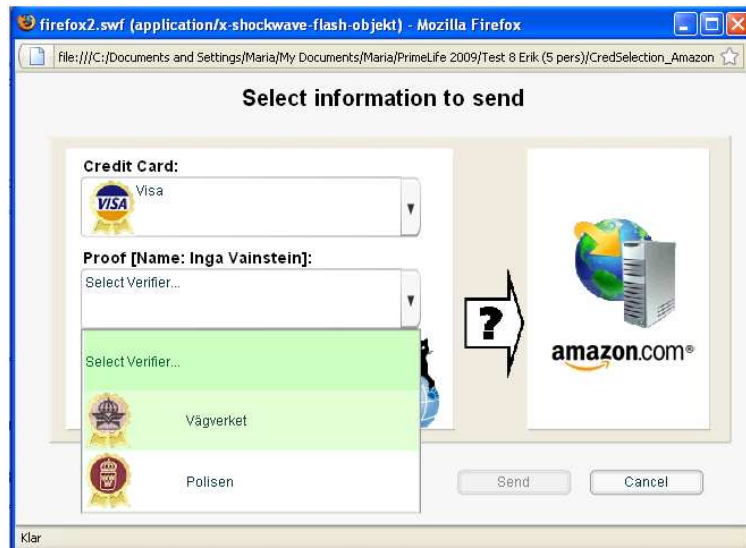


Figure 3: Credential Selection: Attribute-based approach for the second round of tests.

In the third round of tests (Figure 4) we created a hybrid version of the two mental models building on the most positive results of both.

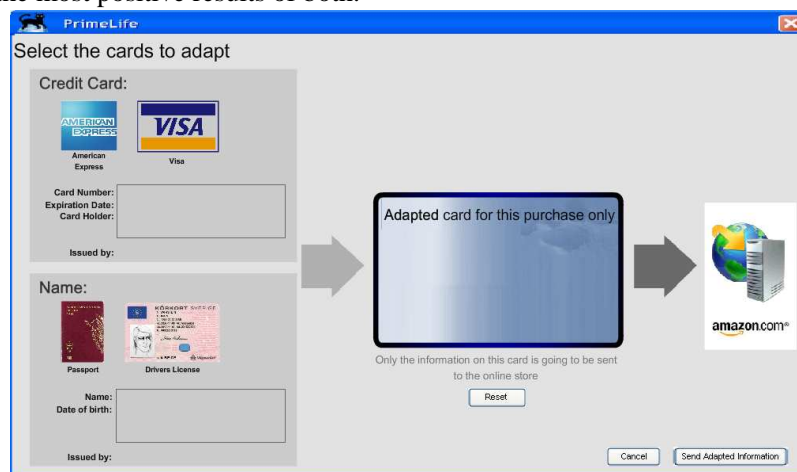


Figure 4: Credential Selection: The adapted card-based approach for the third round of tests, which combines the ideas of the first two rounds.

All tests were performed in a similar fashion. The test users were asked to test a new and more secure payment system where one in addition to a credit card number had to prove possession of a credential with a name that matched that of the credit card. After a brief description of the system they were asked to assume the role of a fictitious person to buy a book from an on-line books store and use the new client for paying for the book of their choice. Having done so, they were asked to report what data they had sent to the vendor as a result of the transaction. In the first round of tests users were presented with a questionnaire containing an image of the source card and a list of possibly sent attributes, they were then asked to mark which of the attributes were sent. During the second and third round of tests, in order not to bias the users towards their experience of plastic cards, users were instead asked to verbally relay what attributes were being sent.

In the card based approach the users (n=39) were told that the fictitious person had imported two identity credentials, a passport and drivers license, and they were to select one to prove their name. In order to show that not all data on the source card was being sent we tested a number of

different GUIs, for example, blacking out the non-relevant information (see Figure 2), greying out everything but relevant data, and using small animations where the relevant data were cut out from the source card and transferred to a new ‘virtual card’ (see Figure 1). All in all during the card based approach 82 per cent of the users made errors of addition i.e. overestimated the amount of data being sent, with an overwhelming majority of these users believing that all data of the source card had been sent. Of the remaining users, six per cent correctly completed the task while the remaining nine per cent made errors of omission i.e. underestimating the amount of data being sent. Interestingly enough a number of users reported that the sent information included their image and written signature clearly showing that they equated the digital credential with the physical one they possessed.

The main difference between the tests based on the card metaphor and the attribute metaphor lay in the description of the system. As the main issue was that users did not understand that only certain attributes were selected from the source card the users were told that the system contained validated attributes of information imported from the Swedish passport authority and the Swedish road authority. Additionally the GUI was changed in order not to show any full cards but rather the information about to be sent (something which was also tested in one of the card based approach test rounds). The results showed that of the users (n=48) now only 33 per cent made errors of addition, 21 per cent made errors of omission, and 46 per cent understood that their name and the issuer of the credential was being sent. In regards to the errors of addition, the most commonly added piece of information was the personal number used in Sweden for nearly all purposes of identification. A number of users also interpreted the instruction to ‘select verifier’ of an attribute as meaning that the information would be routed via the issuer, e.g., the Swedish police and that they would be able to log the transaction.

The third round of tests (n=16) was based on the most positive results of the previous tests, i.e., the low levels of errors of omission in the card based paradigm and the low levels of errors of addition in the attribute based metaphor. As the results of the attribute based approach showed the benefits of moving users out of the current understanding of plastic cards we introduced the concept of adaptable cards. We enforced the idea of adaptability to ensure that users got the message that they were handling credentials that would not behave in the same static fashion that ordinary plastic credentials do. The results showed that only 31 per cent of the users made errors of addition while 56 per cent made errors of omission and 12 per cent fully comprehended what data had been sent. The results show that by highlighting the concept of adaptability, the users’ mental models of the application and understanding of the data minimisation property of anonymous credentials rose while errors of additions fell from 86 to 31 per cent. The results also show an increase in errors of omission from 9 per cent to 56 per cent which obviously is an issue that needs further investigation.

	Omission	Correct	Addition
Card-based	9% (3)*	6% (2)	86% (30)
Attribute-based	21% (10)	46% (22)	33% (16)
Adapted Card-based	56% (9)	12% (2)	31% (5)

Table 1: Proportions (and count) of errors of omission, correct responses and errors of addition in the card based approach, the attribute based approach, and the adaptable card approach

\* Note, the very low rate of errors of omission in the card-based approach might be a result of respondents checking everything on the form rather than understanding the amount of meta data being sent.

In sum, the results of the three rounds of tests regarding a selection mechanism for anonymous credentials show that the data minimisation properties are very difficult to show and that users

comprehension of the UIs clearly hinge on the induced mental model. Inducing adequate mental models is however a key issue in successful deployment of novel privacy technologies and thus needs further attention. When it comes to privacy, the effects of incorrect mental models leads to difficulties in using a given application or not being able to take adequate steps in order to protect one's information (for a further discussion of mental models for PETs, please also refer to D4.1.6).

## 2.3 Research Results from the PrimeLife Prototype Evaluation

During the final PrimeLife prototype evaluation CURE evaluated Clique<sup>2</sup>, Dudle<sup>3</sup>, Reputation Management Wiki [PWG10], Privacy Dashboard<sup>4</sup>, and the "Send Data" dialog [AFP11]. An expert evaluation of Scramble! and iterative usability tests of the "Send Data?" dialog were conducted by KAU.

In this Section we will provide a short overview of the results of the evaluation and provide design implications for the prototypes. Detailed results of the evaluation were presented to the PrimeLife consortium in H4.1.3 "User Evaluation Report. The evaluation results and design implications for the "Send Data?" dialog will be discussed in Section 3.2 of Chapter 3, where we report all research results of Work Packages 4.3 (*User Interfaces for Policy Display and Administration*). The "Send Data?" dialog is one of the main interfaces for PrimeLife Policy Language (PPL) engine and a more detailed evaluation was carried out at KAU.

The design suggestions will be presented in the following format:

<b>Issue:</b>	<b>Short description of the issue</b>
Detailed explanation:	A more detailed explanation of the issue
Heuristic:	<p>A list of heuristics out of Nielsen's Ten Usability heuristics [Nie92], which have not or not sufficiently been followed by the current UI design, but should be considered for addressing this usability issue.</p> <p>Generally, heuristics are rules of thumb that, in our case, describe the affordances of a particular system for the users. Heuristics are formulated more generically than usability guidelines. The heuristics by Nielsen, to which we refer to, are also available in Appendix B: Usability Heuristics.</p>
Severity:	<p>Severity of the issue found. The severity level bases on the effect the issue has on the usability. It was therefore divided into two groups:</p> <p>Major: From usability point of view, we consider that this issue is necessary to be solved in order to make all functions of the system well usable for the majority of users including non-expert users.</p> <p>Minor: From usability point of view this issue should preferably be solved to further enhance the system's usability.</p>
Proposed solution:	A description of proposed solutions for mitigating the issue. If useful a screenshot is also provided. (Please note that these solutions were

---

<sup>2</sup> <https://clique.primelife.eu/>

<sup>3</sup> <https://dudle.inf.tu-dresden.de/privacy/>

<sup>4</sup> <http://www.primelife.eu/results/opensource/76-dashboard>

however not evaluated with end users yet).

### 2.3.1 Demographic Data

On CURE's side, 16 participants, drawn from CURE's test subject database, participated in the final usability evaluation of the PrimeLife Prototypes.

Eight of the 16 participants in Austria were female, 8 male. The participants were between 23 years and 57 years old. When recruiting the participants we looked that they covered a broad age range, since PrimeLife prototypes should be useable for everyone. Seven participants had a university degree; the other nine volunteers completed high school.

Our participants used various browsers (multiple answers were possible) when surfing the Web. Their favourite browser was Firefox with 12 nominations, followed by the Internet Explorer with eight nominations. Chrome was mentioned three times, Opera twice and Safari only once.

Each evaluation slot was scheduled with 90 minutes. We evaluated the prototypes in random order, because experience showed that users are more concentrated in the beginning and some users are slower and therefore it is sometimes necessary to skip tests. The number of evaluations done for each prototype is depicted in Table 2.

In the beginning participants filled out a demographical questionnaire and a declaration of agreement for recording their test session. For each prototype, we introduced the objective of the prototype and gave them about three minutes to become familiar with the prototype. From our experience we know that three minutes are sufficient and that after three minutes participants starts to flutter.

Next they had to solve various tasks with the prototype and think-aloud while interacting with it. After each prototype participants had to fill out the so-called PET-USES (see Section 2.1) and also a questionnaire which dealt with their experience with the prototype such as, "Did you have any problems dealing with it?"

Prototype	Clique	Dudle	Reputation Management Wiki	Send Data	Privacy Dashboard
Number of Evaluations	14	16	13 <sup>5</sup>	14	15

Table 2: Number of evaluations per prototype

### 2.3.2 Clique

Clique is a social network service that provides advanced features for setting access rights for single users, a group of users or all members of the social network (see Figure 5). Clique uses so called "Faces", for enabling users creating various profiles with different access rights, e.g. one profile for friends, one for co-workers and so on.

For evaluating Clique, we prepared a demo account for our participants, which was registered to our PrimeLife Persona Inga Vainstein, c.f. [PriPer]. Since Clique is a very complex application we only tasks were conducted which were accomplishable for participants even without much knowledge of Clique.

---

<sup>5</sup> Two evaluations with this prototype were skipped because of non-working eye-tracking.

Users had to conduct several tasks such as creating a new Face, adding contacts to this Face and writing a new blog post. We decided for these tasks because from our point of view, these are common tasks when dealing with a social network and must also be solvable for new users. This was necessary because our users did not have previous knowledge concerning Clique; neither was it possible to conduct a more detailed evaluation within the scope of this final evaluation.



Figure 5: Clique: Screenshot of Inga's User Profile (Image was cut at the grey-red line for displaying the parts of the UI with which the user has to interact.)

### 2.3.2.1 Results

In general, our participants were able to use Clique, but nevertheless various usability problems were uncovered and became obvious during the evaluation. Nevertheless, most problems would only require small changes of the UI and functionality of Clique, which can – from an HCI point of view - improve the usability of Clique. All of our suggestions for improvements bases on common HCI knowledge.

Main problems (summary):

- After creating a new face the user saw an overview of her faces where she can either enable or delete them. Users had problems understanding the enable functionality.
- Adding a contact
  - Participants had problems understanding the “invite contacts” label. Most of them thought that they can add a Clique member to their friends list, while the functionality behind this label was inviting a new member to join Clique.
  - Participants looked for the possibility for adding a new contact to their friends list in the collection wizard and in the contact collection menu. Both things do not provide the necessary functionality for adding new contacts.
- When writing a poll the Publish button was on the position near the left upper corner of the text entry field. Participants looked for this button on the right side below this field.
- The drag and drop functionality when adding contacts to a collection as well as when defining access rights for a poll was not obvious for our participants. We observed many problems when they first encounter this functionality at Clique.

### 2.3.2.2 Design Implications

In this Section, we summarize the usability issues found during the usability evaluation and make suggestions for improvements.

<b>Issue:</b>	<b>Participants had problems understanding the meaning of the “Enable” button</b>
Detailed explanation:	The enabling of a newly created Face is part of the workflow. Nevertheless, users had problems understanding why it is necessary to enable a face and why there is no possibility for disabling (the label always says enable).
Heuristic:	<i>Efficiency:</i> The enable button confused the test participants which had a negative influence on users’ efficiency. <i>Memory Load:</i> Users are forced to remember if they already enabled a face, since no feedback is given. <i>Task Orientation:</i> Users are forced to enable a newly created face instead of just using it straightforward.
Severity:	Minor Issue
Proposed solution:	Faces should be enabled automatically (default value), see Figure 6. Provide disable functionality.

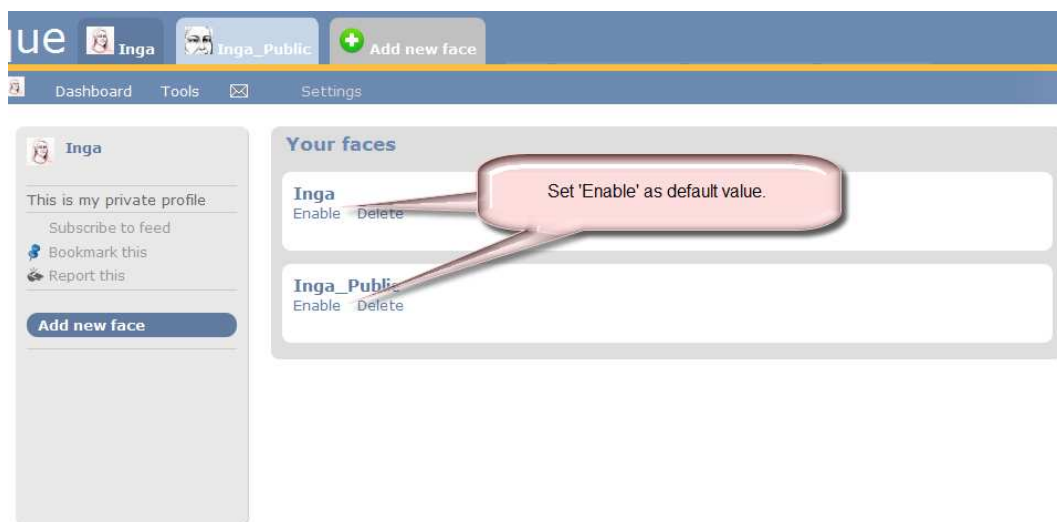


Figure 6: Clique: Enabling a Face

<b>Issue:</b>	<b>Difference between Contact and Members</b>
Detailed explanation:	Participants had problems differing between Contacts and Members.
Heuristic:	<i>Wording:</i> The difference between Contacts and Members was not obvious to the users. <i>Memory Load:</i> Users had to remember / learn what Contacts are and what Members are.



Severity: Major Issue

Proposed solution: Use other labels for Contacts and Members, see Figure 7. We suggest to use “My contacts” and “Members of Clique” to make the difference more obvious.



Figure 7: Clique: Labelling of Contacts and Members

**Issue:** The labeling “Invite contacts” was misleading for our participants

**Detailed explanation:** Participants had problems understanding the label “Invite contacts”. In their point of view the functionality behind the label would enable adding new friends to their contact list. While it currently allows users to invite contact via mail.

**Heuristic:** *Wording:* The used labels are not clear.  
*Memory Load:* Users have to remember which functionality is behind a certain label.

Severity: Major Issue

Proposed solution: Change the “Invite contacts” label to “Invite contacts via E-Mail”, see Figure 8.

Make “Contacts” and “Contacts of” visually better distinguishable, as it is not clear what the difference is.

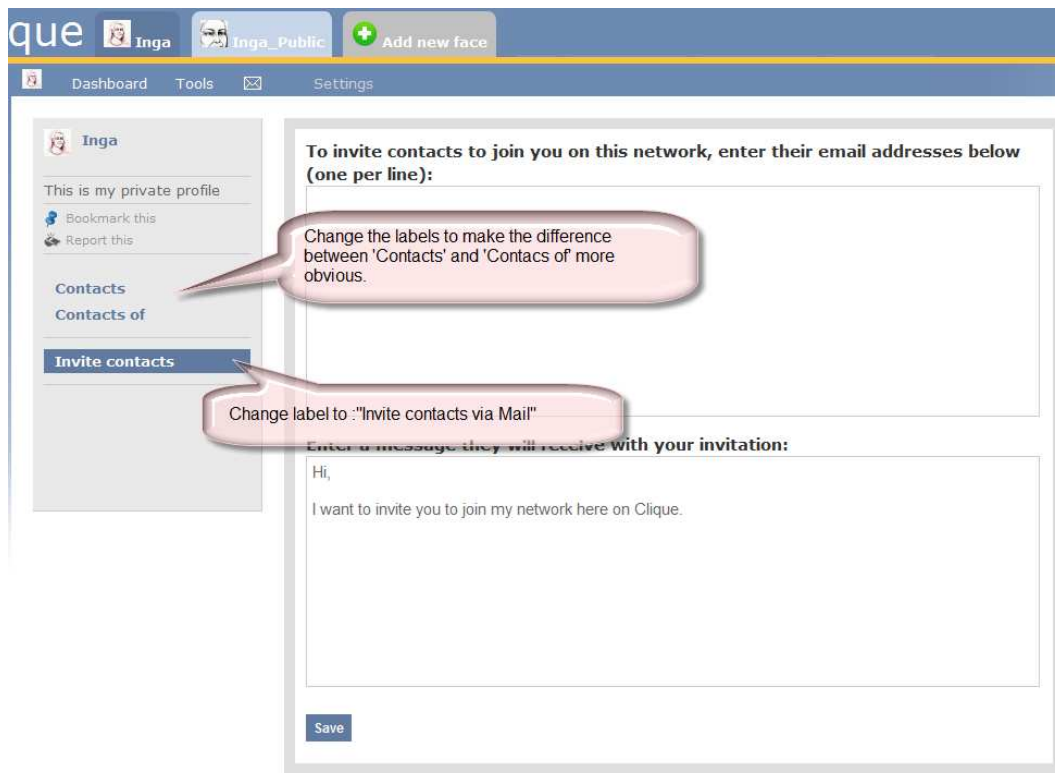


Figure 8: Clique: Invite Contacts Label

<b>Issue:</b>	<b>Adding new members to collection</b>
Detailed explanation:	Participants had problems adding new members to their collection. They looked for such a possibility in the collection wizard or in the contact collection menu.
Heuristic:	<p><i>Efficiency:</i> Confusing interaction is needed for solving this task. This reduces the efficiency of the user.</p> <p><i>Flexibility:</i> Inexperienced users would find adding new members unintuitive.</p>
Severity:	Minor Issue
Proposed solution:	<p>Provide the possibility for adding contacts directly after the collection wizard is finished.</p> <p>Provide at least instructions on how to add a member into the contact collection (like it can be done for inviting new contacts), see Figure 9.</p>

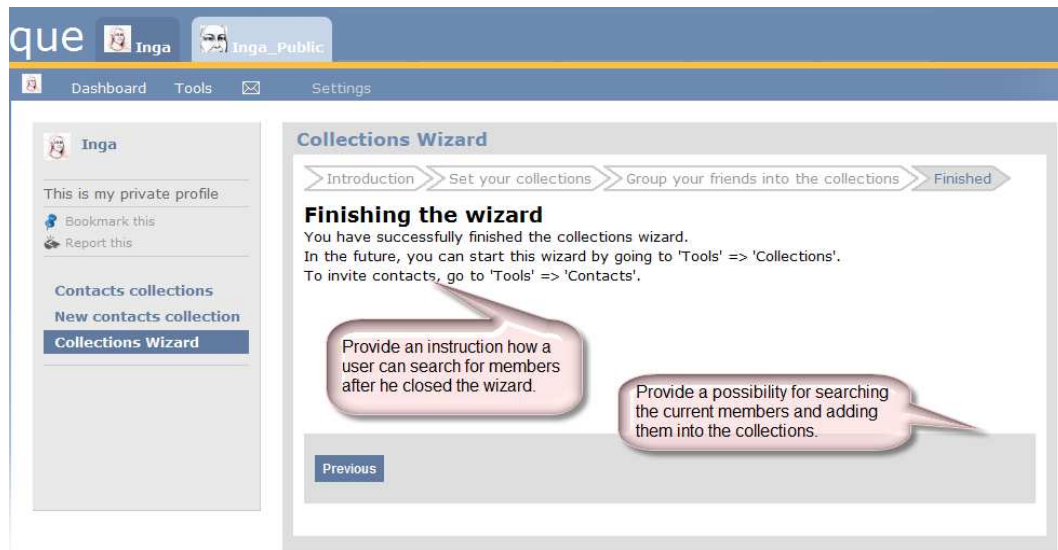


Figure 9: Clique: Add members after the collection wizard is finished

<b>Issue:</b>	<b>Wrong position of the “Publish” button when creating a new blog</b>
Detailed explanation:	The “Publish” button for creating a new blog is in the upper left corner. Participants had problems finding this button.
Heuristic:	<i>Consistency:</i> The position of the button is not consistent. In other parts of the programs the button for the next step (e.g., next windows of the collection wizard) is in the lower right corner (e.g., collection wizard).
	<i>Task Orientation:</i> Users are not able to solve this task straightforward.
Severity:	Minor Issue
Proposed solution:	Put the button below the input boxes, see Figure 10.

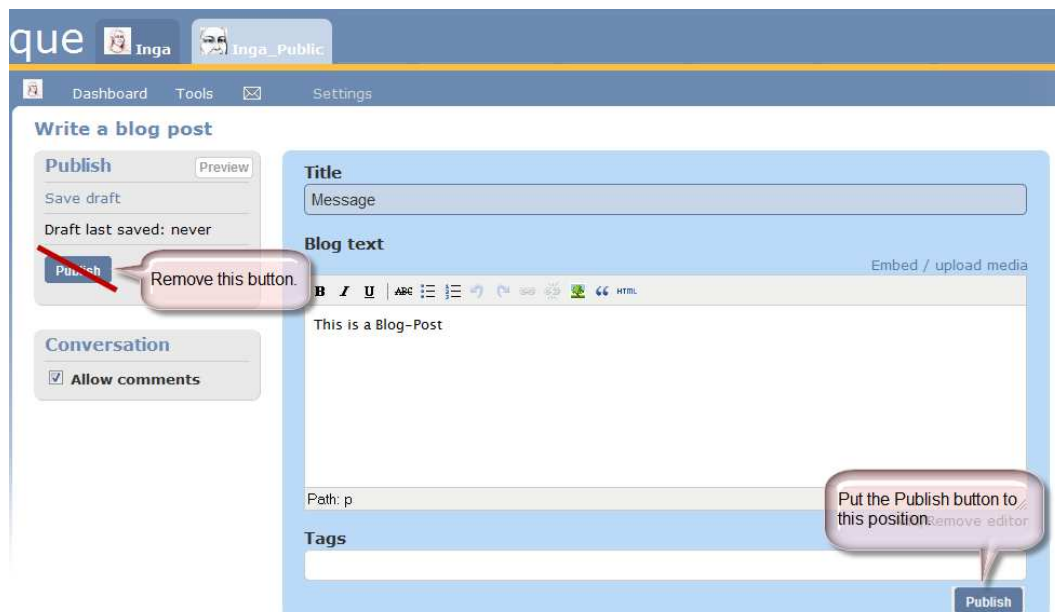


Figure 10: Clique: Publish Button

**Issue:**

**Obviousness of the Drag and Drop functionality**

**Detailed explanation:**

Participants had problems using the drag and drop functionality because it was not obvious for them. Furthermore drag and drop is only possible when dragging the cross on the right side of the suggested collections, see Figure 11.

**Heuristic:**

*Efficiency:* Confusing interaction possibility reduces the efficiency of the users.

*Feedback:* Users do not get feedback to how to interact with the drag and drop boxes.

**Severity:**

Minor Issue

**Proposed solution:**

Best practice solution: Use a parts selector<sup>6</sup> instead of the drag and drop functionality, see Figure 11.

(Alternative: Make the drag and drop functionality more obvious by making the whole box drag-able.)

<sup>6</sup> <http://www.welie.com/patterns/showPattern.php?patternID=parts-selector>

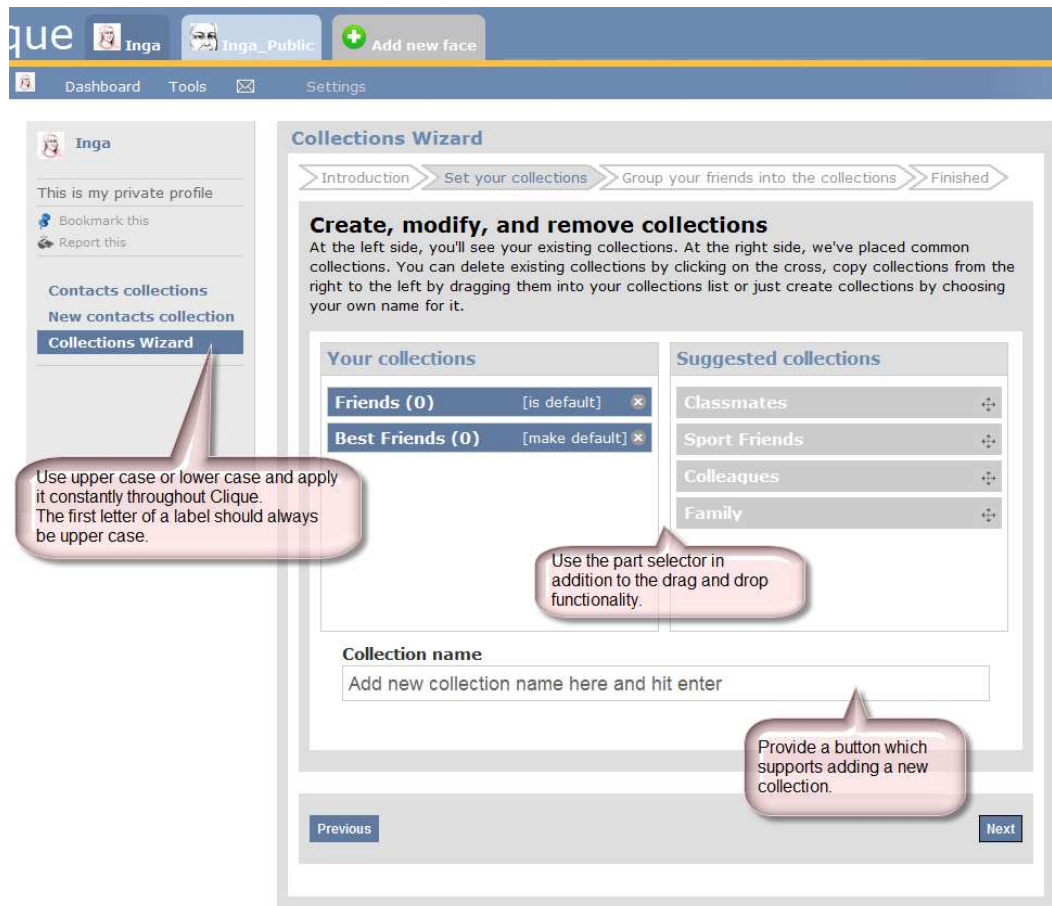


Figure 11: Clique: Drag and drop functionality

<b>Issue:</b>	<b>Enter button is missing when creating a new collection</b>
Detailed explanation:	Problems occurred when creating a new collection (not in the suggestions).
Heuristic:	<p><i>Aesthetics and emotional effect:</i> Users are forced to read the text in the collection name field. If they do not read it they will not be able to solve this task, which frustrated the users.</p> <p><i>Flexibility:</i> Users did not find the needed interaction intuitive.</p> <p><i>Feedback:</i> No feedback is given that pressing enter is needed for adding a new collection to the list.</p> <p><i>Memory Load:</i> Users are forced to remember the text in the collection field.</p>
Severity:	Minor Issue
Proposed solution:	Put a button next to the text field which the label “Add collection” or “Create collection”. Nevertheless provide also the functionality of the enter key, see Figure 11.

### 2.3.2.3 Final remarks

Clique is based on the open-source social network engine Elgg<sup>7</sup> and some occurring problems were part of Elgg. Nevertheless these problems need to be compensated since users do not differ between Elgg and Clique, for users a prototype works or it does not work. From HCI point of view the usability of Elgg needs improvements because only than a framework basing on this tool would be really useable.

Even though Clique was considered as usable by the test participants, the above mentioned improvements for Clique can increase the usability of the software and can therefore potentially also increase the acceptance.

### 2.3.3 Duddle

Duddle is a privacy-enhanced event scheduling tool (e.g., “When should we meet?”). Additionally to event scheduling, the application can be used to create more general polls (e.g., “What kind of food do you prefer?”). Duddle enables participants to vote anonymously and uses asymmetric cryptography and anonymisation techniques. This ensures that (1) individual votes are authenticated and (2) users' preferences are encrypted and therefore anonymised. For more detailed information about the Duddle protocol, please see [KB09, Ke11].

In order to use the scheme, a key-pair has to be generated within the Duddle-Web interface.

Duddle was evaluated with 16 participants. The tasks for this prototype were designed in cooperation with the developer. The tasks were embedded into a small scenario, in which some friends try to organize a reunion meeting. The people writing the e-mails which contain the tasks are the PrimeLife Personas [PriPer]. This reunion meeting context fostered the understanding of the users and created a more natural situation for using the tool.

Figure 12 shows the main page of Duddle.

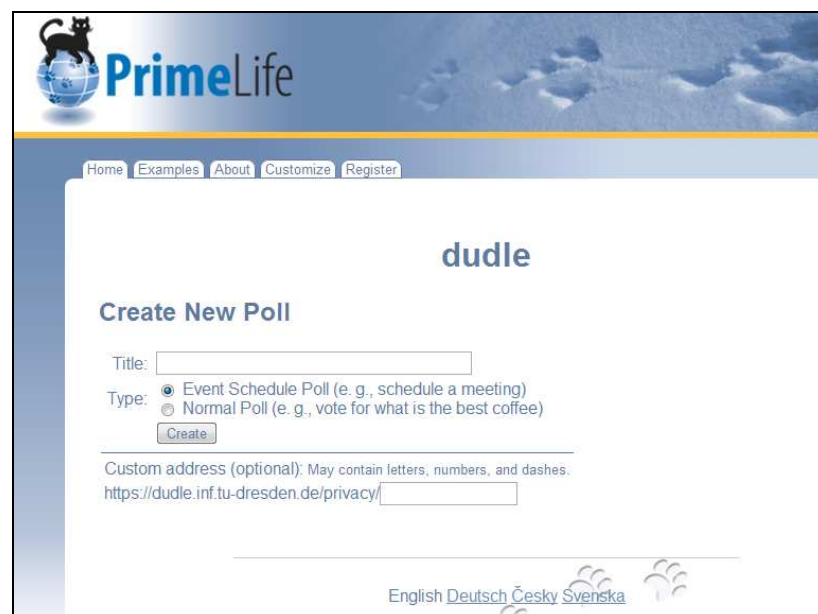


Figure 12: Duddle: Main Page

---

<sup>7</sup> <http://www.elgg.org/>

### 2.3.3.1 Results

In general our participants were able to handle Dudle. Nevertheless some problems occurred when they dealt with the tool.

First of all participants did not comprehend the (meaning of the) key. The complex idea of the system was not understandable for them. Some also mentioned that they would prefer creating their own password instead of a generated key.

Furthermore the test supervisors detected various problems concerning the registration (e.g., tab was not obvious), the invitation to a poll or the enabling of anonymous voting.

Some participants did not comprehend the blue dots, see Figure 16 in the anonymous voting polls and the label “add columns”, see Figure 15.

### 2.3.3.2 Design Implications

In this Section we provide design implications for Dudle basing on the results of the usability evaluation.

<b>Issue:</b>	<b>Problems understanding the key</b>
Detailed explanation:	During the test it became obvious that users had problems understanding the meaning of the key and why it is better than a password. For our participants the key was just a long chain of number and characters.
Heuristic:	<i>Efficiency:</i> Users had problems understanding the key metaphor, which has a negative influence on its efficient use. <i>Transparency:</i> Users have no indication why the key is needed and what it is doing.
Severity:	Major Issue
Proposed solution:	Present the meaning of the key in a more understandable and visible way for users, e.g., through a short introduction why it is better than a password.  Make it transparent to the user, why the key is more secure than a password, see Figure 13.

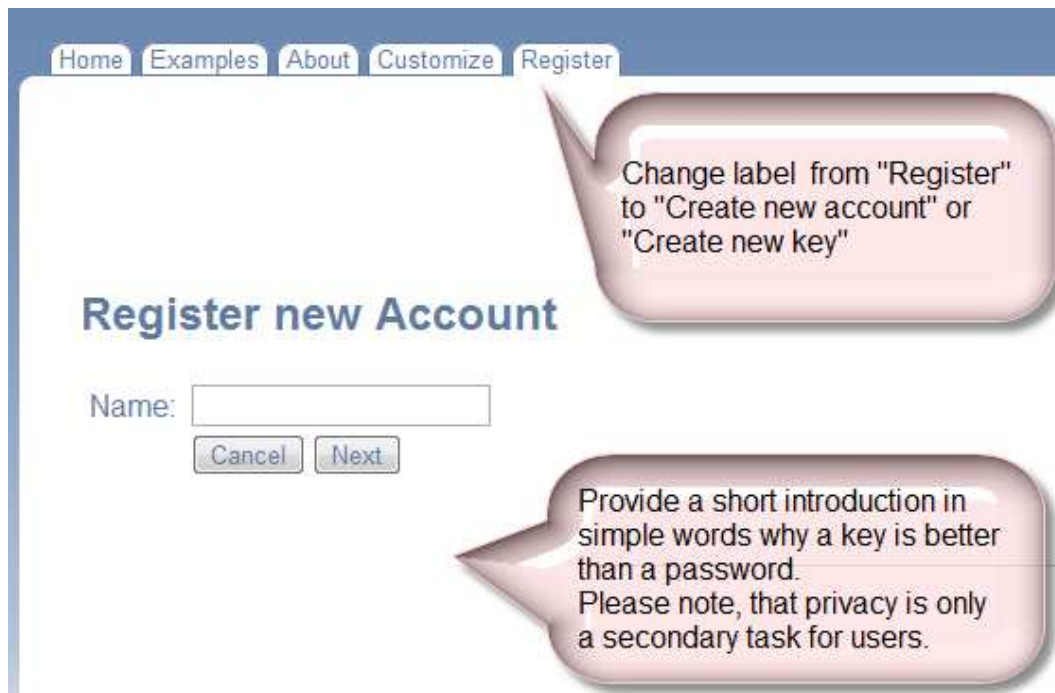


Figure 13: Duddle: New Account

<b>Issue:</b>	<b>Registration tab</b>
Detailed explanation:	Some participants did not see the registration tab on the first glance.
Heuristic:	<i>Task Orientation:</i> The current organization of the tabs is not obvious
Severity:	Minor Issue
Proposed solution:	Make the registration more obvious for participants. Provide an option "New here? Create your key" on the main page (Home tab).
<b>Issue:</b>	<b>Create new poll - button</b>
Detailed explanation:	On the "create new poll" screen the alignment of the UI elements is puzzling: The "create" button is before the possibility of entering a custom address.
Heuristic:	<i>Aesthetics and emotional effect:</i> The missing button under the custom address field has a negative emotional effect on participants since it is not obvious how they can submit their entry.  <i>Efficiency:</i> Confusing button positions reduce the efficiency of users.  <i>Task Orientation:</i> The position of the buttons is not ideal.
Severity:	Major Issue
Proposed solution:	Put the button under the custom address field (see red arrow in Figure 14)



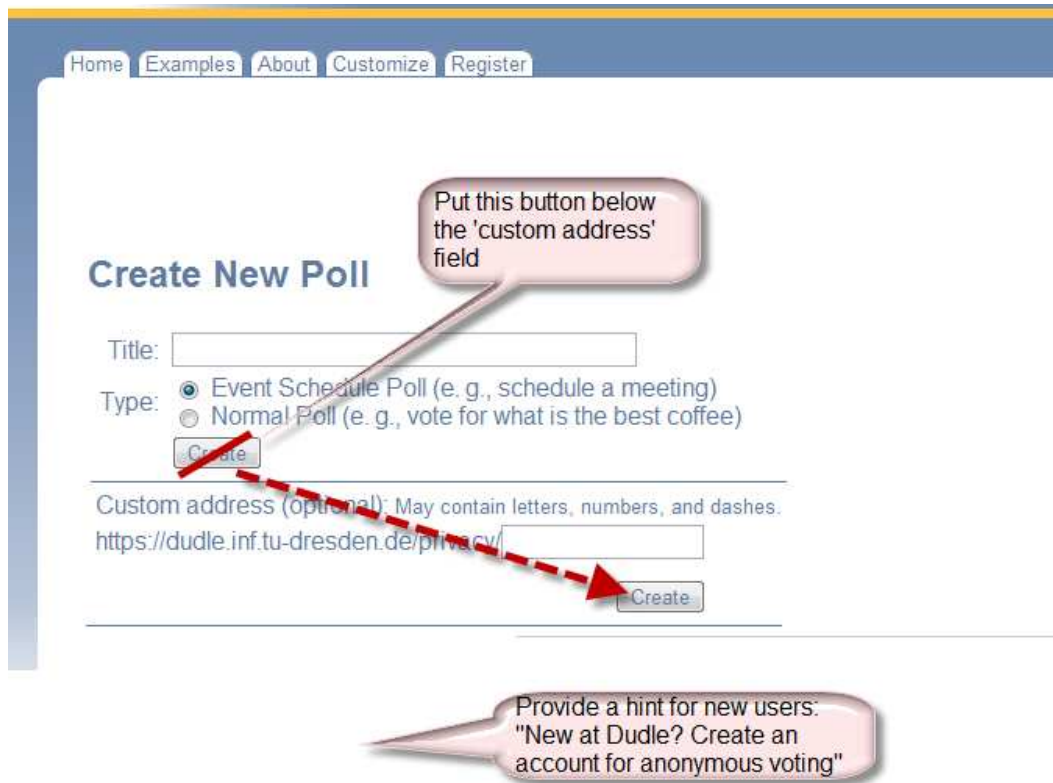


Figure 14: Duddle: Create Button Position

<b>Issue:</b>	<b>“Add columns” label</b>
Detailed explanation:	Participants criticized the “Add columns” label. For them adding a new column was related to spreadsheets and software like Microsoft Excel. Furthermore participants stated that they are entering new options and not new columns.
Heuristic:	<i>Wording:</i> This term was not clear for participants.
Severity:	Minor Issue
Proposed solution:	Change the label into “Options”, since the input represents the various available options in the poll, see Figure 15.

## Add and Remove Columns

Enter all alternatives (columns), you want to ask the participants of the poll. The participants will state one vote for every alternative you give here separately.

Alternative:

Description (optional):

## Preview



Change label 'columns' to 'options'.

Figure 15: Duddle: Columns vs. Options

### Issue:

### Usage of blue dots for presenting an anonymous vote

#### Detailed explanation:

The blue dots were not understandable for our test users. For them it was not obvious that a blue dot indicated that a user had already voted anonymously.

#### Heuristic:

*Memory Load:* The used icon (blue dot) is not obvious and not explicit enough.

#### Severity:

Major Issue

#### Proposed solution:

Change the color of the field from blue to gray (no access / not available) and use another Icon, e.g., a crossed eye.

Furthermore in the “Last Edit” column a value should be added which indicates that this user has already voted anonymously, e.g. “Done”, see Figure 16.

		Mar 2011			Apr 2011				Last Edit
		Thu, 31			Fri, 15				
Name		14:00	15:00	16:00	11:00	12:00	13:00	15:00	
  Ines		✓	X	?	X	✓	X	?	22.03.12:29
  Frank		✓	X	?	X	✓	X	?	22.03.12:29
Hannes		*	*	*	*	*	*	*	
  Inga		—	—	—	—	—	—	—	
		 ✓	 ✓	 ✓	 ✓	 ✓	 ✓	 ✓	
<input type="text"/>		 X	 X	 X	 X	 X	 X	 X	<input type="button" value="Save"/>
		 ?	 ?	 ?	 ?	 ?	 ?	 ?	
Total		2	0	0	0	2	0	0	

Provide information in the "Last Edit column" that Hannes already voted. e.g. "Done".

Change the colour from blue to gray (inactive) and add an icon instead of the dots, e.g. a crossed eye.

Figure 16: Duddle: Feedback anonymous voting

**Issue:**

**Checkbox for enabling anonymous voting**

Detailed explanation:

Participants did not activate the checkboxes for anonymous voting. Since anonymous voting is one key-feature of Duddle this boxes should be checked by default. Furthermore the checkboxes should be enabled for clicking.

Heuristic:

*Efficiency:* The inactive check-box has negative influence on the task efficiency of the user. Participants of the study did not see the pencil which enables the changing of the “Vote anonymously” state, c.f., Figure 17.

Severity:

Major Issue

Proposed solution:

Checkboxes should be enabled (clickable). Furthermore the checkbox should be activated by default as one can assume that one wants to vote anonymous when there is a registered user with the name.

## Invite Participants

The screenshot shows a web interface for inviting participants to a poll. It features a table with columns 'Name' and 'Vote Anonymously'. The table lists four participants: Inga, Hannes, Frank, and Ines. Each row has a hand icon, a checkbox, and a name. The 'Vote Anonymously' column has checkboxes, with the first two checked and the last two unchecked. Below the table is a text input field containing 'Ca' and 'Carol', and an 'Invite' button. At the bottom are 'Previous', 'Next', and 'Finish' buttons. Three callouts provide feedback: one points to the 'Vote Anonymously' checkboxes, another points to the 'Invite' button, and a third points to the text input field.

Name	Vote Anonymously
Inga	<input checked="" type="checkbox"/>
Hannes	<input checked="" type="checkbox"/>
Frank	<input type="checkbox"/>
Ines	<input type="checkbox"/>

Ca  
Carol

Previous Next Finish

Invite

Check boxes should be activated to change selection.

When adding a registered user activate the anonymous voting by default.

Before inviting the first participant provide the hint "Invite yourself to enable anonymous voting".

Figure 17: Duddle: Invite Participants

<b>Issue:</b>	<b>Participants did not invite themselves to a poll</b>
Detailed explanation:	Participants did forget to invite themselves to a poll or did not understand why this should be necessary.
Heuristic:	<p><i>Efficiency:</i> Inviting oneself to something is an unintuitive interaction in real-world.</p> <p><i>Memory Load:</i> Users are forced to remember to invite themselves to the poll.</p> <p><i>Transparency:</i> Users do not know that they have to invite themselves to a poll.</p>
Severity:	Major Issue
Proposed solution:	Provide a hint in the text field in which users have to enter their name, see Figure 17. Also, adding the user to the poll by default could be a solution.

<b>Issue:</b>	<b>Link to the poll is not clickable</b>
Detailed explanation:	After creating a new poll, the link is not clickable.
Heuristic:	<p><i>Efficiency:</i> Inconsistent interaction prevents users from achieving tasks efficiently.</p> <p><i>Memory Load:</i> Users are forced to copy the poll to the task bar if they want to have a look at it.</p> <p><i>Task Orientation:</i> Users expect that a link is clickable.</p>

Severity: Minor Issue  
Proposed solution: Make the link clickable, see Figure 18.



Figure 18: Dudle: Clickable Link

### 2.3.3.3 Final remarks

In general our participants were satisfied with Dudle (average satisfaction: 2.25; 1=very high, 5=very low). Nevertheless, implementing above mentioned suggestions for improvements will increase the usability of the tool.

### 2.3.4 Reputation Management Wiki

The Reputation Management Wiki implements a privacy awareness panel (c.f. Figure 19) for a Wiki [KPS11], [BPL11], [D2.3.1]. The main objective of the privacy awareness panel is to support users about their potential audience when disclosing data. The privacy awareness panel is also described in [PWG10], but in the context of a web forum.

The goal of this evaluation was to test, if users notice the panel and whether they understand the content of the panel. For the evaluation we did not use any tasks but asked the user to click through the available prototype. We used eye-tracking to evaluate if participants recognized the panel.

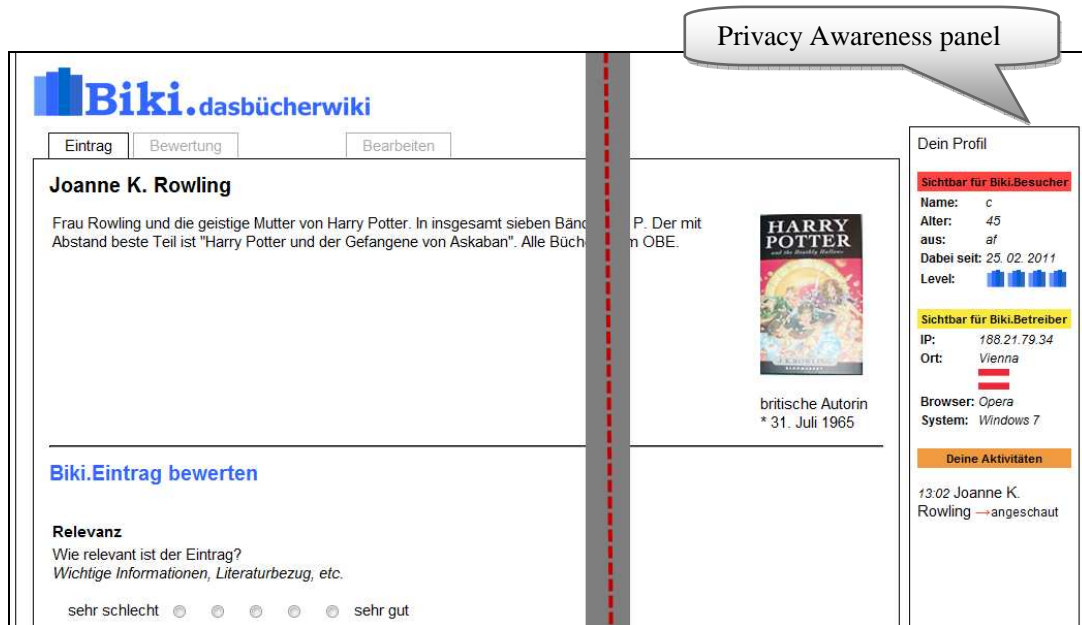


Figure 19: Reputation Management Wiki: User Interface (Image was cut at the grey-red line for displaying the important parts in this deliverable)

### 2.3.4.1 Results

The most interesting observation is that the results of the eye-tracking indicated that all 12 participants looked at the privacy awareness panel approximately 30% of total time viewing this page (see also the eye-tracking heat map in Figure 20).

Nevertheless, nine of them stated in the questionnaire that they did not notice the privacy panel and become only aware of it at the end of the evaluation when the test supervisor called their attention to it. Nevertheless, none of our participant stated that he had problems understanding the content and the meaning of the display after their attention was brought to it.

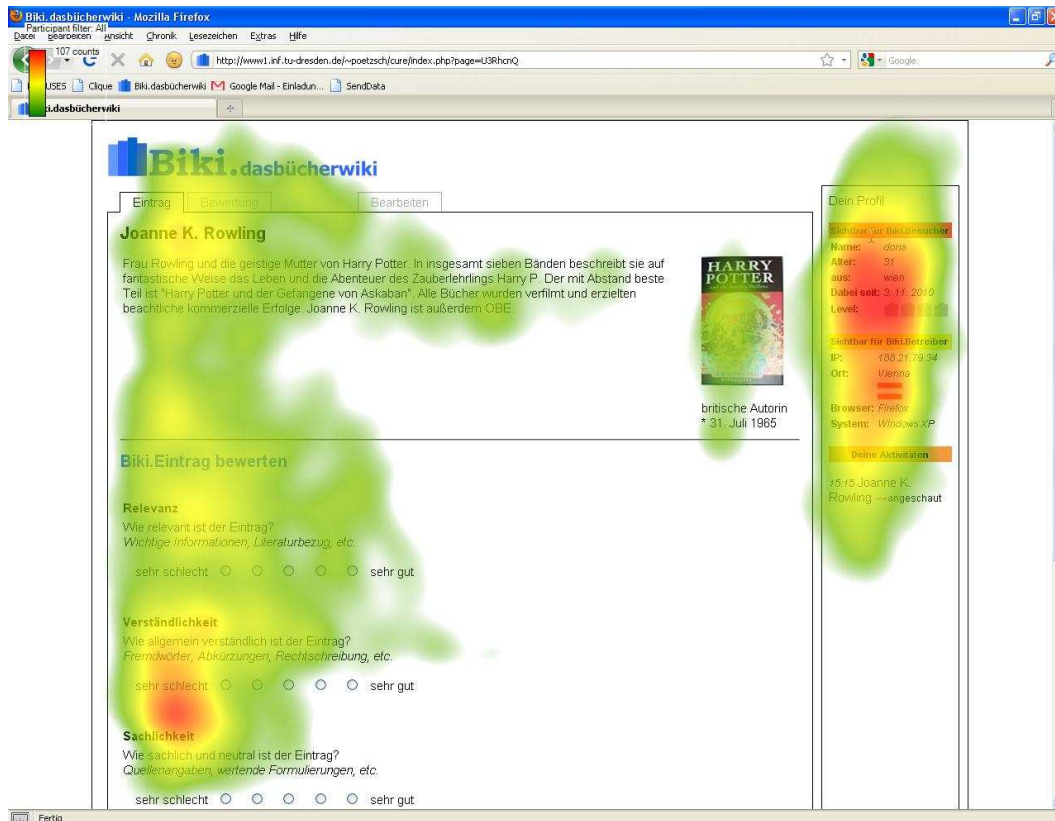


Figure 20: Reputation Management Wiki: Heat map

### 2.3.4.2 Design Implication

While all participants looked at the panel only three stated that they were aware of its content. The others looked at it were not conscious of it. As design implication we suggest to make the panel and its content more eye-catching, e.g., through a privacy indicator, which shows how privacy aware their settings are.

Very positively was that participants stated that they had no problems understanding the content of the panel.

### 2.3.5 Privacy Dashboard

The Privacy Dashboard is a Firefox plugin, which includes a light version of the “Data Track”, which helps the user to track what data is collected by the visited websites. It also provides the possibility to set privacy preferences for each visited site, see Figure 21.

15 participants evaluated the Privacy Dashboard. During the test, participants had to conduct several tasks such as changing privacy preferences, finding out more about the website and also conducting a query in the Data Track.





Figure 21: Privacy Dashboard

### 2.3.5.1 Results

During the evaluation of the prototype, only a few problems occurred but these problems were observed by many participants:

- After executing a Data track query, participants had problems understanding and interpreting the results
- Participants were unsure whether their changes in their privacy preferences were saved because no save-button was available.
- Problems occurred with the understanding of the purpose of the “Check site” buttons.

### 2.3.5.2 Design Implications

In this Section we describe more details of the issues that we found and provide suggestions for solving these issues.

<b>Issue:</b>	<b>Query results are not understandable</b>
Detailed explanation:	The results of the query were not understandable for our users. At the moment the results are not understandable for regular users.
Heuristic:	<i>Memory Load:</i> Results of the query are not easy to understand and no help functionality is provided.  <i>Wording:</i> The choice of terminology might not be understandable for all users.
Severity:	Major Issue
Proposed solution:	Present the results in the user's language. Figure 22 shows an example for query results. Especially in the name and value section



use meaningful names, instead of “js\_stats” you could e.g., use “statistical values”.

Provide a help function explaining the used terms.



Figure 22: Privacy Dashboard: Query results

Issue:	Missing Save button at current website tab
Detailed explanation:	Participants were unsure whether their settings where stored after they clicked on “Simplify my choices”.
Heuristic:	<i>Feedback:</i> Users do not get any feedback whether their choices were stored.
Severity:	Minor Issue
Proposed solution:	Solution 1: Provide a “save“ button below the website preferences, see Figure 23. Solution 2: Provide a hint that the settings where stored.



Figure 23: Privacy Dashboard: Preferences

<b>Issue:</b>	<b>Meaning of “Check site” buttons</b>
Detailed explanation:	Problems occurred with the understanding of the meaning of the check site buttons.  It is also not obvious that a click on the buttons opens an external website.
Heuristic:	<i>Memory Load:</i> Users are only able to find out the functionality of the check site buttons through try-and-error principle.  <i>Aesthetics and emotional effect:</i> It is not obvious where these buttons are belonging to.
Severity:	Major Issue
Proposed solution:	Provide a visual separation between preferences and “check site” buttons. Provide a short outline which describes the purpose of the buttons, see Figure 24.

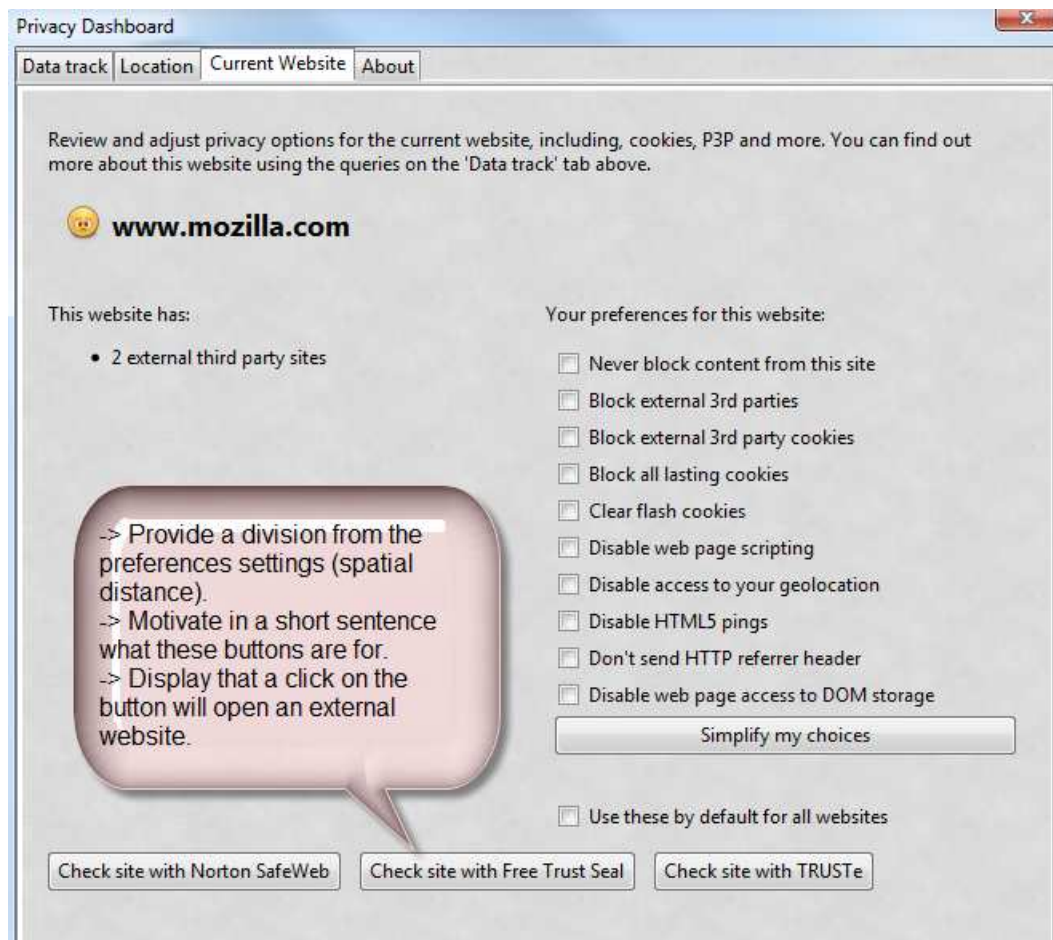


Figure 24: Privacy Dashboard: Check Site Buttons

### 2.3.5.3 Final remarks

The average satisfaction of our participant with the Privacy Dashboard was 1.85 (1=very high, 5=very low). Some test users even asked whether the tool is available for their personal use.

### 2.3.6 Scramble!

The idea of Scramble! is to provide users with control over their own data when using Social Network Sites. “Its main target is to protect users from sharing sensitive information with Social Network Sites (SNS) providers” [Pri10c]. In this sense, Scramble! allows people to share their postings with friends and other individuals with the right cryptographic key, while at the same time keeping these postings private from other unauthorized users and the Social Network Site itself. Scramble! includes a series of features, such as “broadcasting” encryption for multiple recipients and listing “tiny urls” instead for large encrypted blocks of text.

An expert UI evaluation of Scramble! was carried out at Karlstad University with the purpose of recognizing the major usability flaws and discovering ways in which its interface could be improved. A full usability evaluation was not considered appropriate for this prototype since its was not at a mature enough state of development. Even though the prototype contained all the essential functionality from the requirements, its usability remained quite undeveloped, probably due to the fact that its development team failed to get input from usability experts at an earlier

stage and delivered an already established design concept. It was considered that carrying out a usability tests with the proposed interface would have returned invalid or insignificant results. We decided therefore to provide recommendations for UI improvements that should be implemented before conducting usability tests. It is desirable for the design of Scramble! to be made in a way that average, non-expert users are able to understand it and adapt it easily to their daily usage of social networks.

### 2.3.6.1 Design Implications

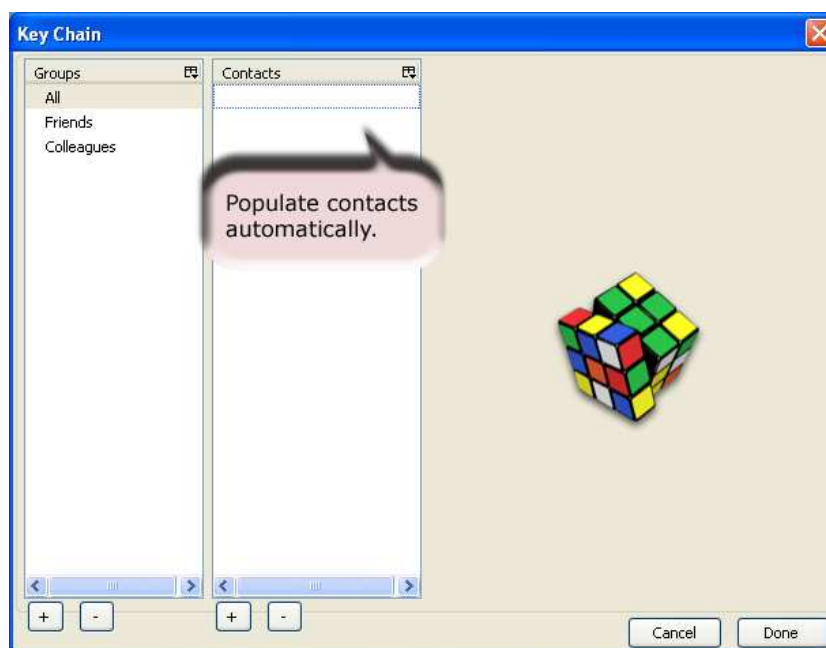


Figure 25: Scramble!: No possibility to populate contacts automatically

<b>Issue:</b>	<b>No possibility to populate the list of contacts automatically</b>
Detailed explanation:	No possibility to populate the list of contacts automatically. Users have the burden of creating key pairs manually.
Heuristic:	<p><i>Flexibility:</i> Inexperienced users would not find the program intuitive.</p> <p><i>Memory load:</i> Users are forced to remember their list of friends and their information in order to find the prototype usable.</p> <p><i>Wording:</i> Cryptographic terms are usually unfamiliar to users who are not interested in cryptography or computer security.</p>
Severity:	Major Issue
Proposed solution:	Provide the feature of extracting the list of contacts from different Social Network Sites. Users should be able to select those contacts with whom they would like to share encrypted messages by obtaining and saving their public key.

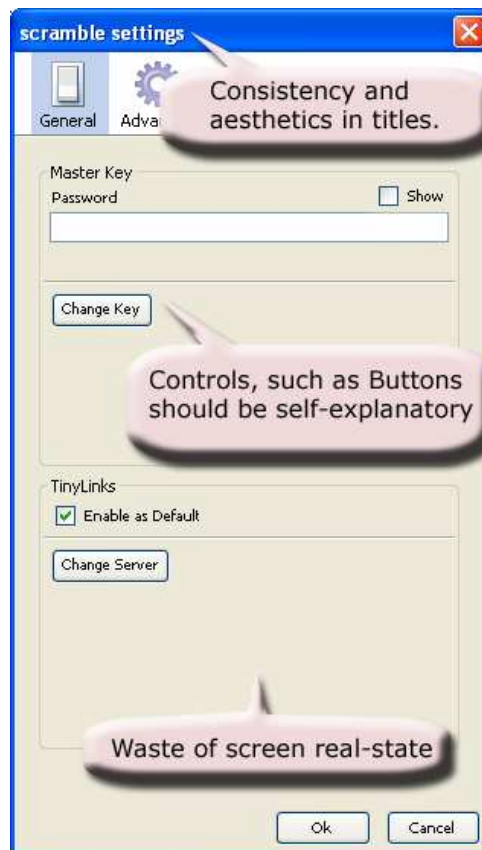


Figure 26. Scramble!: Unintuitive Settings

**Issue:**

**Unintuitive Settings**

Detailed explanation:

The different fields and controls in the Settings dialog are not obvious and can create confusion. No indication is given to users about the changing of some settings.

Heuristic:

*Aesthetics and emotional effect:* Empty space in dialogs is not aesthetically pleasant. Waste of screen real-state.

*Efficiency:* Confusing controls and terms reduces the efficiency of users.

*Feedback:* Changing or selecting some settings does not fulfill users' expectations on how the program should react. No visual feedback is given indicating that changes have been applied.

Severity:

Major Issue

Proposed solution:

Provide another mechanism for setting up the system at the beginning, such as a wizard, and structure the interface in a more consistent way. The installation of a usable program should be as seamless and intuitive as possible.

**Issue:**

**Accessibility of different features**

Detailed explanation:

Even though Scramble! is a powerful tool offering a number of

features, the user would have a hard time finding and understanding those features.

- Heuristic: *Efficiency*: Unintuitive interactions, such as searching for contacts or encrypting text, prevent users from carry out their tasks efficiently
- Transparency*: Users have no indication of what the program is doing or is able to do, such as selecting embedded text from a website and encrypting/decrypting it.
- Severity: Minor Issue
- Proposed solution: Make a more logical context menu as well as a general menu where the users can have access to the different features offered by Scramble! Having some kind of “help” or information via tooltips would help users understand more the different elements of the interface.

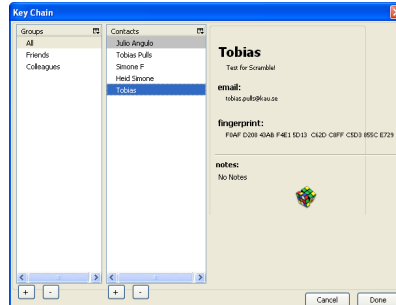
- Issue:** Complicated use of expert terminology and security concepts
- Detailed explanation: At the same time, average users are not familiar with cryptographic terminology and the concept of key pairs or key chains.
- Heuristic: *Wording*: The program uses too much cryptographic terms that are not understood and unintuitive for the average user.
- Severity: Minor Issue
- Proposed solution: Change the term to be more general and understood by average users and not only computer security experts. Information should be presented in a general way in which users will understand its immediate benefit.

- Issue:** **Consistency in wording and interaction paradigms**
- Detailed explanation: The different dialogs, wording, and interaction paradigms are inconsistent throughout the application.
- Heuristic: *Consistency*: The title in the dialogs are not consistent. The flow of interaction is not consistent either.
- Efficiency*: Inconsistent interaction prevents users from achieving tasks efficiently.
- Wording*: The program uses too much cryptographic terms in an inconsistent way.
- Severity: Minor Issue
- Proposed solution: Restructure each of the dialog windows so that they are consistent across the whole program.

The user opens the “Crypto Dialog”, pastes some text and clicks on the “Encrypt to Link” button.



The “Key Chain” window opens, where presumably the user can select a contact to exchange the message with and press “Done”



The user is taken back to the “Crypto Dialog” with an encrypted string (when it works!!)

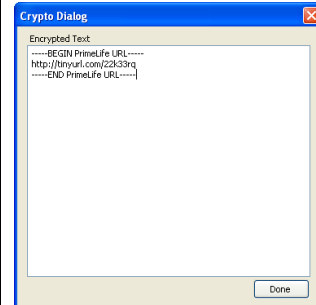


Figure 27. Scramble!: Confusing interaction flow in the Crypto Dialog and Key Chain editor

## Issue:

## Confusing interaction flow in the Crypto Dialog and Key Chain editor

### Detailed explanation:

Encrypting and decrypting text are essential features of Scramble! The way of achieving encryption via the so called Crypto Dialog does not have an optimal flow of interaction. The Key Chain Editor’s buttons “Cancel” and “Done”, there are some situations in which they appear to have the same effect.

### Heuristic:

*Efficiency:* The way dialog windows close down and pop-up hinders users from encrypting text in an efficient way.

*Task orientation:* The sequence in which dialogs are presented is not optimal.

*Wording:* The choice of terminology might not be understandable by all users.

### Severity:

Minor Issue

### Proposed solution:

The interface can be structured in a way in which the user is taken in more logical steps between selecting a text to encrypt, selecting the contacts’ keys, and then the program returning the encrypted text to the user.



Figure 28. Scramble!: Obscure search functionality

**Issue:**

**Obscure search functionality**

**Detailed explanation:**

The search function provided in the Key Chain window is not at all intuitive. It does not provide any level of transparency in the sense that the user does not know where the search is being performed or what the progress of the search is (i.e. not appropriate feedback). The search is done against some remote server which is completely unknown to the user. The user is not informed on the range of the search that she can perform (e.g., can the user perform a search with all existing names and email addresses, or only with names and email addresses of a certain Social Network Site?).

**Heuristic:**

*Control:* Users lose control over where the interaction takes place.

*Feedback:* No clear indication given that a search is been done.

*Transparency:* Users do not know how and where the search is been done.

*Task orientation:* Way of searching for contacts does not provide an optimal interaction or user experience.

**Severity:**

Major issue

**Proposed solution:**

Make it clearer that the search is being perform against one key server, let the user choose how to perform the search. Improve the search functionality to be responsive and more accurate, so that users know that something is going on and that their searches actually return valid results.

## 2.3.6.2 Final remarks

The concept provided by Scramble! prototype is very appealing, powerful and could provide a good privacy-friendly addition to Social Networking Sites. However, an improvement to the



usability issues of Scramble! listed above can bring an improvement in its efficiency and make it more appealing for average, non-expert users.

### 2.3.7 Conclusions

In general the evaluated prototypes were accepted well by our participants. However, our results indicate that improvements are still needed. Our participants were able to handle the current versions of the prototypes, but minor changes and adoptions would improve the usability and workflow of all prototypes.

An interesting finding of the evaluation was that the acceptance of the applications (Privacy Dashboard, “Send Data?” dialog (see also Section 3.2)), which support users in their daily life in the web, was higher than the acceptance of specialized applications such as Clique, Duddle or the Reputation Management Wiki. We presume that participants saw higher advantages of general applications for their daily online life.

# Chapter 3

---

## Research Results – User Interfaces for Policy Display and Administration

---

Privacy policies are an important means for making the data handling practices of services sides more transparent and thus can help users to do well-informed decisions in situations when they are requested to disclose personal data in exchange for a service. Privacy notices posted on web sites are often not comprehensible to end users. Privacy policy engines based on machine-readable privacy policy languages, such as PPL (PrimeLife Policy Language), aim at making the core information of privacy better comprehensible. For this, the user-friendly user interfaces for displaying and handling privacy policies are needed.

PrimeLife WP4.3 (“*User Interfaces for Policy Display and Administration*”) has investigated how to simplify privacy policy administration and negotiation and how to present policies to end users in a user-friendly manner. In this Chapter, we report about the recent research results of WP4.3 in the area of privacy policy icons (Section 3.1) and in the area of user interfaces for policy administration and display, which we designed, tested and implemented for the PPL engine (Section 3.2). The objective of this Chapter is to complement previous PrimeLife publications on WP4.3’s results in the deliverable D4.3.2 [Pri10d] and in the PrimeLife book [AFP11].

### 3.1 Policy Icons

#### 3.1.1 Introduction

Every person has an individual view on her privacy, what to protect and what information to share with others. Using the World Wide Web many individuals are not aware of who is collecting and handling their data for what purpose. Due to the fact that effective protection of informational privacy requires clarity on the data processing and possible consequences, transparency is a core element of data protection. Supporting transparency, icons could be used to illustrate certain aspects of data handling that today may be described in lengthy, hard-to-read privacy policies only. In general, content that should be quickly understood by a broad audience is often expressed via icons, e.g., symbols pointing to fire exits or subway stations. Well designed icons to convey information by means of a single graphical representation expressing the relevant content in an understandable manner for wide audiences, ideally even across cultural domains. Privacy icons

should therefore offer at least some valuable information on a first-glance basis for users and point out core issues related with the processing of data in a given case.

Within the PrimeLife project, privacy icons have been developed inspired by other researchers trying to find best fitting icons for illustrating important aspects of privacy-relevant data handling and data processing. First results of this research have been published in the PrimeLife deliverables D4.3.1 [FiWäZ09] and D4.3.2 [FiZ10] as well as in [HNH11]. Based on the results of user tests and thought-provoking impulses from related work, the PrimeLife project has worked on a final proposal for privacy icons to be demonstrated below.

### 3.1.2 Related work

The idea of illustrating privacy aspects with icons is a common idea and has been developed earlier within the privacy community - many researchers worked on this idea. "Privacy icons" are thereby understood as simplified pictures expressing privacy-related statements [HNH11]. Various areas of use can be distinguished [Ha09]:

1. statements on results of data protection audits or similar evaluations concerning informational privacy-relevant components of data processing, e.g., privacy seals or trust marks,
2. statements on how well a situation matches the privacy preference of a user, e.g., Cranor's Privacy Bird for P3P [Cra05] or the Privacy Nutrition Label by Kelley [KBCR09] also for P3P policies,
3. statements from privacy policies on planned or performed processing of potentially personal data or on guarantees concerning the use of these data, e.g., proposals from Rundle [Run06], Mehldau [Meh07], Helton [Hel09], Raskin [Ras11] and Pinnick [Pin11] as well as the evaluative approach in the KnowPrivacy report [GPS09] and Cooper's W3C Privacy Ruleset [Co11],
4. statements on how personal data may be used by others, e.g., Bickerstaff strengthening the user's perspective and proposing "Privacy Commons" analogue to "Creative Commons" [Bic08], an icon set tailored to users in social networks by Ianella and Finden [Ian10], or the Privicon proposal enabling senders of e-mails to express how they wish that recipients should handle the message [Pri10].

The sets differ in respect of the targeted use cases. Another differentiation could be made concerning the underlying understanding of privacy or the understanding of privacy in the jurisdiction of origin. Here the ideas proposed by Rundle [Run06] have a strong focus on US-American perspectives, depicting rights that are granted by EC law anyhow and are thus in theory not necessary to make explicit within the European Union.

### 3.1.3 The early PrimeLife icon sets

To date, two icon sets had been developed within the PrimeLife project. The first approach of PrimeLife in the first year of the project intentionally had a broad scope including icons for three different categories: icons representing processing steps, icons representing data types, and icons representing groups of recipients [FiWäZ09]. A complete overview on this icon set is given in PrimeLife deliverable D4.3.1 [FiWäZ09]. This icon set was tested internally, the results of this test led to the further development of the second icon set.

The second approach of PrimeLife icons in the second project year contained two different categories: icons for general usage, and icons for usage in Social Network Sites (SNS). The icon set for general usage in turn included icons for data types as well as icons for processing steps or

an e-commerce scenario [FiZ10] and was tested externally by KAU and CURE. The KAU test was performed with Swedish and Chinese students, the CURE test with a wider group of participants from Austria, Germany and Switzerland. Some of the test results will be shown more precisely below; an overview about the KAU test and the second PrimeLife icon set is provided in PrimeLife deliverable D4.3.2 [FiZ10].

### 3.1.4 Test results

The two different icon sets developed in the first two project years both base on the idea of trying to visualise many different aspects with icons. Thus they include a huge number of different icons for different purposes. As mentioned above, the first icon set [FiWäZ09] differentiated between the following three categories: icons representing processing steps, icons representing data types, and icons representing groups of recipients. Evaluating this approach, the icon sets have been tested. In addition to the evaluation of each individual icon, the general approach of using many different icons was evaluated. The first icon set was only tested internally and revealed shortcomings when displaying a large variety of purposes for different use cases by too many icons. All results of this internal test led to the second icon set. Based on the first icon set, the second icon set did no longer differentiate between three categories, but addressed general usage on the one hand and specifically social network sites on the other.

This second icon set has been tested externally. Karlstad University performed a test with about 17 Swedish and Chinese students, CURE performed a bigger online test with about 70 participants from Austria, Germany, Switzerland and other countries. While the participants in the CURE test assessed themselves as being privacy-aware, the students were not specifically aware of privacy issues. The combination of both test results therefore offered a good cross section about the potential user group. In the CURE survey the participants were offered 2 or 3 different icons that should have the same meaning; the participants had to evaluate which of them fits best to a described use case.

An overview about the comprehensive test results can be found in IFIP/PrimeLife SummerSchool Proceedings 2010 [HNH11].

The results of the tests illustrated different results. Some icons have been rather well-rated in both user tests; they got an acceptance rate of more than 50% for their understandability. Some of them (for the data type “personal data”, the purpose “shipping”, the data type “payment data”, “selected individuals” in Social Network Sites, the purpose “user tracking” and the data type “medical data”) are shown in Figure 29:



Figure 29: Excerpt of well-rated icons

Different results were achieved for example for the "Storage" icon, see Figure 30. While the KAU participants (university students) rated this icon quite well, the same icon failed in the online test due to the fact that a floppy disk was seen as a very outdated symbol for data storage and therefore cannot be a seminal icon.



Figure 30: Storage icon

The test results also show that some processing steps, data types and recipient groups are hard to illustrate. For instance, the proposals for icons with the meaning "Friends" and "Friends of friends" as a potential recipient group in Figure 31 and Figure 32 all failed in the user tests.



Figure 31: Excerpt of low-rated icons for "Friends of friends"



Figure 32: Excerpt of low-rated icons for "Friends"

Especially the failing of all "Friends" icons was surprising due to the fact that some SNS like Xing use similar symbols to illustrate a users' list of contacts and as the concept of friends and followers is known in the widely used SNS.

In general, special recipient groups in SNS seemed to be hard to visualise. Only the icons representing "selected individuals" and "public" were well-rated here - maybe due to the fact that they did not attempt to illustrate special groups of recipients, see Figure 33.



Figure 33: Excerpt of well-rated icons for the recipient groups "Selected individuals" and "Public"

However, it is not possible to take all well-rated icons (e.g., those shown in Figure 29) to design a final PrimeLife icon set: Some of them could illustrate certain aspects quite well, but these aspects may be too specific for a usage in a small icon set. For instance, an icon expressing a data type as the "financial data" icon could be used as illustrative elements for a privacy policy, but then other data type icons would be necessary, and this again would call for a larger icon set. On the other hand, users usually are aware when they enter financial data, and today these data are hardly disclosed automatically by the user's browser. So this well-rated icon is not really needed in a minimised icon set.

Anyhow, the test results suggest that clear icons with few details are preferred.

These results combined with the requirements for a widespread usage of icons led to the final PrimeLife proposal.

### 3.1.5 Requirements for widespread usage

Obviously, privacy icons have to fulfil several requirements if they should be successful in enhancing the clarity of data processing and privacy-related statements [Ha09]. Privacy icons should allow for quick comprehension by all possible groups of users regardless of their cultural or social background. Different individual, cultural, societal or legal constructions of privacy and individual freedom should not hamper grasping the meaning of icons. Social factors like education and age must not restrict their user-friendliness. Furthermore, it should be possible to understand the icons across different legal framework [HNN11]. Therefore, a successful and generally intelligible design of icons is a prerequisite for a widespread usage.

Besides, another prerequisite for a widespread usage of icons will be the interest of the users regarding their content: privacy icons might be successful if they are able to display information users care about, but are not aware of without the usage of icons. When designing icons on data processing, it should be avoided to patronise the users which might happen if they do not only convey a neutral statement, but express a warning: For icons being used in specific privacy software, a warning functionality can be desired if the data processing is not privacy-friendly, and of course the user may choose to be warned if a setting does not match her configured preferences. But for global use and acceptance by the data controllers and data processors the icons should describe what happens to the users' data in a neutral way. The icon sets should aim at enhancing transparency for the users so that they are able to decide upon the information conveyed by the icons.

Note that the situation the user is acting in influences what she is interested in: For a user visiting a website while surfing the net, it might be of special interest whether IP addresses, cookies or data from the browser are being stored, how long they are stored, how they will be analysed for what purpose, whether there is third party tracking or whether data might be passed on by the data processor. Also, data concerning behavioural targeting and targeted advertising can be relevant from the user's point of view. All this information might be interesting for users in an e-commerce scenario, too, but in addition information on the account handling, ways of processing the address or banking data and safeguards to guarantee a specific level of data security come into the focus.

Even with the best design of icons, the distribution of icons and their implementation won't happen on its own. Today, there are not many incentives for most website operators to install icons: In general, putting icons on a website can cause costs because they have to fit into the layout, there has to be process to guarantee that the icons are up-to-date, and they may provoke questions by users or competing website operators if there is the slightest possibility that the icons are not perfectly understood or even considered misleading. Even with a design as neutral as possible, privacy advocates would give recommendations which icons may stand for not so privacy-friendly practices. This means that there can be an incentive for privacy-aware website operators who want to express their privacy compliance or privacy-enhanced settings, but definitely not for the other operators. In case the distribution of icons reaches a critical mass which could be supported if global players adopt icons for their websites, companies not using any icons would stand out negatively, and the absence of privacy icons could become a warning flag [Ras11].

However, at least for the area of online behavioural advertising there might be another incentive, at least for the European context: In 2010, the Article 29 Working Party has issued a working paper on online behavioural advertising where the usage of icons is commented as follows: "Network providers/ publishers should provide the information directly on the screen, interactively, if needed, through layered notices. In any event it should be easily accessible and

highly visible. Icons placed on the publisher's website, around advertising, with links to additional information, are good examples. The Article 29 Working Party urges the network providers/publisher industry to be creative in this area." [WP2/10]. The necessity for placing a well visible icon has been taken up from the European Privacy Seal initiative EuroPriSe as one criterion that has to be fulfilled for being awarded a privacy seal [Euro11]. These approaches may lead to a state-of-the-art for implementing icons at least for the area of online behavioural advertising.

In addition, a push for icons may come from third parties that rate or describe website practices (e.g., [GPS09]) or from software developers when designing browsers and browser plug-ins as well as identity management or privacy tools.

In any case, the international standardisation of the design and the semantics of icons used alone and, if possible, in combination is desirable, so that there is clarity both for users and data handling parties on the meaning and possible rights or obligations that are related to the use of icons.

### 3.1.6 The PrimeLife icon approach

The development of icons and their evaluation within the PrimeLife project and the thought-provoking impulses from other icon developers [Run06] [Meh07] [Bic09] [KBCR09] [Hel09] [Ras11] [GPS09] [Pin11] [Co11] have influenced PrimeLife's final proposal for privacy icon sets. In particular, the objective for the last project year was to reduce the variety of icons and limit the contexts of use. This may ease the implementation of website operators and enhance the acceptance of users, especially in an introductory phase where further experiences can be collected before icons may become widely standardised.

To start with, PrimeLife proposes two icon sets: The first icon set should give information about the website's data handling (cf. Subsection 3.1.6.1), and the second one should address data disclosure in social network sites (cf. Subsection 3.1.6.2). Subsection 3.1.6.3 will mention additional contexts where the icons may be useful.

#### 3.1.6.1 Information about the website's data handling

Within PrimeLife the terminology "digital footprint" had been defined as data created by tracking the primary user's behaviour while surfing the net or a specific website. Thus, the PrimeLife project illustrated how tracking could be realized in a privacy-preserving way and which requirements have to be fulfilled, (cf. PrimeLife Heartbeat H1.3.5 [StHaRa09] and PrimeLife Deliverable D4.3.1 [FiWäZ09]). The importance of this topic is illustrated in the ongoing public debate. The recent discussion on "Do Not Track"<sup>8</sup> for a universal web tracking opt-out has awakened attention of users because many of them feel uneasy about being tracked, but only few have been aware of tracking. So PrimeLife considers this field as relevant for introducing a small icon set that might be picked up in the ongoing discussion. The icon set should cover an information that data are being stored and how long, whether data are being passed on, whether a website uses third party tracking, and whether behavioural targeted advertising is in place. The respective icons are visualised in Figure 34.

---

<sup>8</sup> <http://donottrack.us/>.



Figure 34: Proposal for PrimeLife icons

The semantics of these icons are explained in the following:

- **"Data are being passed on" icon**

The "data are being passed on" icon illustrates the fact that personal data may be passed on by the data handling organisation. This might happen as renting or selling of the personal data to third parties such as marketing partners or corporate affiliates and subsidiaries [GPS09]. The icon should not comprise the exceptional and usually not preventable possibility that data controllers have to transfer data to third parties where required to do so by law, or where such third parties process the data on the data controllers' behalf which means that the data controllers maintain their responsibility regarding data protection law.

For many users the fact that data may be passed on to third parties will be surprising. So, this information should enable the user to decide herself whether she wants to use a service that probably passes on her data or not, or whether she wants further information (provided via mouse-over functionality or a mouse click).

- **"Storage period" icon<sup>9</sup>**

The "storage period" icon contains two different statements: firstly, the fact that data will be stored, and secondly, the storage period. If the time of the storage period is given, this also means that the data will be deleted after this period, so there is implicit information that the data won't be stored forever and that the data processor has implemented a process for deleting the data after the given time.

Within the PrimeLife project it was discussed whether a static current value to visualise this should be used or a dynamic one. We decided not to overcrowd this icon and therefore chose a static one. Alternatively, a symbol for an hourglass or an analog clock could also be used to illustrate the current value.

When using this icon, the data for which the storage period is given has to be clearly identifiable by the users. This could, e.g., be the IP address, cookies or browser chatter, a chatroom posting, or even data given in an e-commerce scenario that might be tax-relevant and demand longer storage periods.<sup>10</sup> Further, the purpose of the data storage should be made transparent to the user. This additional information should be provided in a text available via mouse-over functionality or being presented if the user clicks on the icon.

---

<sup>9</sup> A similar icon has been proposed by [Meh07].

<sup>10</sup> For example, in Germany tax-relevant data usually have to be stored for 10 years (see section 147 ff. Abgabenordnung (AO), the German tax code), while other data might only be stored for other periods (see inter alia retention periods for companies during their warranty periods or legally obliged data retention, see Directive 06/24EC).



- **"(Third party) tracking" icon**

The "(third party) tracking" icon stands for different variants of user tracking, i.e., possibilities to follow the user by her digital "footprints": Each time a user visits a website, the server automatically collects certain information about the visitor, including, e.g., the user's web browser, the operating system, the IP address, the visiting time and possibly cookies. The cookies' lifetime can last for the session only, or it can be much longer in case of a persistent cookie. In this case, the storage period could be added via using the "storage period" icon shown above. In addition, the purpose for the tracking could be given, e.g., whether it is a website-only tracking to improve the site or customise it to better fit individual users' tastes, or whether the tracking data is used by third parties to place advertisements.

Note that the icon proposed by [GPS09] looks similar, but is restricted to third party tracking for placing advertisements only: "site allows third parties to place advertisements that may track user behavior". We propose to differentiate between the tracking and the targeted advertising as described below.

- **"(Behavioural) targeted advertising" icon**

This icon illustrates whether users will be targeted for advertising purposes based on their behaviour. Technically, behavioural targeting works by means of tracking and combining certain information about an individualised user. There is also a risk that profiles created for behavioural targeting may be used for purposes other than advertising. For example, ad networks that focus on something called "re-targeting" may already be using profiles to help advertisers charge different Internet users different prices for the same item. Behavioural profiles, particularly those that can be tied to an identifiable individual, may also be a tempting source of information for companies making decisions about people's credit, insurance or employment [CDT09].

To enable users to give or deny her legally valid informed consent for the usage of cookies for behavioural targeted advertising, the comprehensive information about certain facts is necessary. This includes information about the identity of the data processor, purpose of processing or the retention period to guarantee the necessary transparency thus the user knows about tracking taking place. Here, the icon could be of benefit for service providers to ensure that users become aware of the tracking taking place giving the possibility to look up details in the privacy policy. A given consent may then be considered informed, cf. PrimeLife deliverable D4.3.1 for details about how deployment of privacy icons aids in regard to informed consent.

Today's online behavioural advertising systems track the user's surfing behaviour on a website or across several websites by means of (browser) cookies [Eur11]. The use of cookies is regulated by Article 5(3) of the ePrivacy Directive [EC02/58]. Thus, legal provision for the storage of cookies and gaining access to cookies necessitates the user's prior informed consent, so-called "opt-in" [Eur11].

In "Opinion 2/2010 on online behavioural advertising", the Article 29 Working Party focussed on (future) usage of behavioural targeted advertising. One of the conclusions is that fact that ad network providers are bound by the obligations of Article 5(3) of the ePrivacy Directive insofar as they place cookies and/or retrieve information from cookies already stored in the data subjects' terminal equipment [WP2/10]. Cookie-based opt-out mechanisms in general do not constitute an adequate mechanism to obtain informed user consent. In most cases the user's consent is implied if they do not opt out. However, in practice, very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertising, but rather because they do not realise that the processing is taking place, much less how to exercise the opt out [WP2/10]. Pointing

out relevant information with the "(Behavioural) targeted advertising" icon can provide at least basic information to user. Again, most users won't know whether a website enables behavioural targeted advertising. The "(Behavioural) targeted advertising" icon can express that and thereby offers an informational surplus value to the user. The user can now decide on herself whether she wants to visit such a website or not, and whether she opts out.

It is also conceivable to sensitise the user if the data controller or the data processor have commercial interests in the user's data, but this may be harder to define. Such an icon could be designed as shown in Figure 35.



Figure 35: Proposal for a commercial interest icon

As mentioned above, the icons above only illustrate the existence of special data practices. Thus, for each category a negated icon, i.e., an icon for the negation of a statement that another icon expresses, could also be useful - without the risk of overwhelming the average user. A negated icon could be designed as being crossed out, see, e.g. Figure 36



Figure 36: Proposal for an icon stating that there will be no aggregation with profile data

One problem in displaying information via a crossed out icon could be the clarity of the icon. Due to the fact that the icons won't be large, illustrations within the icon will have to be very clear. In case of crossed out icons this clarity might suffer.

### 3.1.6.2 Information about data disclosure in Social Network Sites

In both former PrimeLife icon sets special icons for usage in SNS were developed due to the fact that SNS become more and more important areas of life for many people - including the forced disclosure of personal data [FiZ10]. Figure 37 shows an overview about icons that could be used for SNS and may provide an informational surplus value for the user.



Figure 37: Excerpt of icons for SNS usage

Due to the fact that other icons for SNS usage failed in the user tests (cf. Section 3.1.4), we focussed on the three icons above in Figure 37 for specific usage in SNS. Reducing the quantity of icons was an objective of the further development, cf. Section 3.1.4.

Especially for specific data items from the user's profile, the recipient groups – i.e., who will be able to access the information as cleartext – are not always clear to the users: Therefore, the "selected individuals" icon can illustrate that certain data disclosed by the user in the SNS will only be visible for selected individuals, e.g., friends or contacts of the user. This could also be helpful to support audience segregation functionalities (if implemented in the SNS) available for example in Clique [BeLe10]. Another possible recipient group is expressed by the "whole net" icon. This icon stands for the fact that certain data disclosed by the user might be visible for every web user. If users are aware of that before disclosing the certain data items, they might be willing to change the recipient group or the data content. A variation could be the "whole net" icon that integrates the logo of a specific SNS: this could mean "whole social network" instead of "whole web".

The "identification" icon belongs to a different category. It means that the user may be identified while proceeding to disclose certain data within the SNS. Especially in a setting of anonymous or pseudonymous usage of a SNS, this information can remind users of an additional risk.

### 3.1.6.3 Further usage possibilities for the icons

Previous work of PrimeLife on icons envisioned further usage scenarios, and the icons from the last icon set as briefly described in this text can be used in these scenarios, too. One possibility is the illustration of elements of a privacy policy, so that users can put their attention directly to those categories that are most interesting for them. Moreover, users can learn about the icons and their semantics, if they appear also in privacy policies - with the possibility of further explanation in text form or in multimedia formats.

A second possibility could be that identity management systems and privacy tools that help users to manage their privacy needs pick up the icons. During the PrimeLife project a prototype of an identity management system was developed [DoBoK10]. The choice of icons could be triggered by third-party ratings (see e.g. [GPS10]) or by machine-readable policy statements from the website. Again, the tools may educate users by giving more explanation on the usage and semantics of the icons.

In case icons become successful, the sets probably will be extended, so that most settings concerning data processing that users may be interested in are covered. To prevent problems for data processors in installing the correct icons, tools such as wizards may help to guarantee that the right icons are chosen and are presented in the right order enhanced by additional information where needed. Such wizards could combine the management of real processes of data handling, the wording of a natural language privacy policy, the statements in a policy language, and finally the choice of icons.

### 3.1.7 Excursus: Privicons

An example for the usage of icons in a peer-to-peer scenario when users themselves attach to their data information on how they want others to handle them is the Privicon approach. The Privicon approach is being developed by researchers of Stanford University, the PrimeLife project and interested individuals [Pri10]. With the Privicon approach, the sender of an e-mail message has a means to express her preferences on how the message content should be handled by the receiving user(s). For this purpose, the semantics of six icons in a graphical as well as in pure ASCII representation ("Privicons") are described. They are illustrated in Figure 38.







 <b>[X] Keep Private</b>	 <b>[=] Delete After Reading</b>
 <b>[o] Keep Internal</b>	 <b>[-] Don't Attribute</b>
 <b>[&gt;] Please Share</b>	 <b>[/] Don't Print</b>

Figure 38: Privicons

These icons can syntactically be integrated in the first line of the body, in the subject line and/or in a dedicated header of any e-mail message.

The six Privicons have the following meaning: By using the "keep private" Privicon, the sender of the e-mail requests the recipient(s) to keep the received message private. Related is the usage of the "keep internal" Privicon by which the receiving users are asked to present the content only to those people that are common friends, or otherwise qualify as "internal", e.g., by being part of a group of people that are in a tight relation to both the sender and the respective receiving user.

In contrast, the "please share" Privicon expresses the sender's desire that the recipients share the content or even the full e-mail message itself with others.

Again, another confidentiality-related Privicon is "delete after reading": The sender requests the recipient(s) to delete the e-mail after reading it. By using the "don't attribute" Privicon, the sender asks the receiving user(s) to not attribute, name or mention the original sender of the e-mail message in any kind. If not stated otherwise, the receiving user(s) may quote, follow or paraphrase the content, facts and opinions voiced in the original message. The Privicon "don't print" describes the sender's request that the recipients do not print the e-mail message.

Meanwhile a first browser extension of the Privicons is being provided via the project's website <http://www.privicons.org/>.

### 3.1.8 Conclusion and outlook

Privacy icons may be important means of conveying relevant information about the processing of personal data to a user and thereby enhance her awareness concerning her privacy. The development of the final PrimeLife icon proposal indicates the further proceeding in the icons development.

Being aware that different research groups work on that kind of privacy icons emphasises the need for standardisation. In parallel to standardisation efforts that, among others, should involve data protection authorities as well as user organisations, the approach of machine-readable privacy statements should be brought forward.

Furthermore, it has to be ensured that users will interpret icons with the same understanding the data processor had in mind when illustrating them. The same applies for the written policy: due to the fact that icons cannot replace a written policy, it has to be ensured that the icons do not suggest other content than the written policy.

The PrimeLife proposal might serve as a basis for developing uniform icon sets that could be introduced by leading providers.

Besides, thought should be given to incentives for data controllers to inform the data subjects in a better way than pointing them to the privacy policy and to educate individuals for better understanding of all aspects that are relevant to their privacy.

## 3.2 Policy Management and Display – 7<sup>th</sup> Iteration cycle

One of the aspects of the PrimeLife project was to technically enforce user control and information self-determination. An important prerequisite for supporting users' control is to make privacy policies of service providers more transparent and understandable.

For achieving better transparency, the PrimeLife Policy Language (PPL), allows users to define and adapt their privacy preferences declaring under which conditions they would like to release what types of personal data. PPL also has the capability of comparing the users' preferences to the privacy policy of a service provider, so that users can be informed about the extent to which their privacy preferences will be satisfied. However, for ordinary computer users, defining and adapting their privacy preferences for properly protecting their privacy online are complex and error-prone tasks which usually require some level of expertise on basic legal privacy concepts and principles. Besides, it is not reasonable to assume that users are willing to spend their time and effort on configuring privacy preferences, specially considering that security and privacy protection are not the users' primary goals [WT99].

For simplifying the management of privacy preferences, work in PrimeLife has proposed an interface called the "Send Data?" dialog, providing users with predefined standard privacy settings which can be customized "on the fly" (i.e., can be modified and saved as a transaction takes place) and assisting them at the moment of selecting certifying attributes that verify their identity.

The "Send Data?" dialog has its origins in the PRIME (Privacy and Identity Management for Europe) project [PFHD+05], where legal and usability requirements were identified for an interface of a user-friendly tool for privacy policies management and administration. Since then, the "Send Data?" dialog has gone through various iterations of development and users' feedback has been considered at every iteration cycle. As of the moment of writing, the dialog is at its 7<sup>th</sup> iteration cycle (Figure 40), which will be the final cycle within the PrimeLife project. Earlier description of the "Send Data?" dialog's interface elements, design decisions and results from usability tests can be found in previous PrimeLife deliverables [Pri09c, Pri10d, AFP11].

As of the 4<sup>th</sup> iteration cycle of the dialog, a few important changes were introduced that have been persistent in the succeeding iterations:

- A two-dimensional "nutrition table" for privacy was introduced to the dialog's interface based on the design suggestions and positive test results presented in [KBCR09]. This suggested table was modified to fit the previously identified legal and HCI requirements and to meet the demands of PPL.
- The use of a *mismatching* icon was suggested as a way to visually indicate, in a not too alarming way, that a mismatch exists between the user's privacy settings and a service provider's privacy policy.
- A user-friendly way of letting users select the credentials that certify the attributes requested by a service provider and enter values for uncertified attributes. This mechanism for credential selection is based in a card-based approach, as explored in [Pri10b].
- An easier way to change privacy settings by providing "standard" predefined privacy settings which can be customized semi-automatically "on the fly", assisting users to state their preferred level of privacy depending on the scenario of the transaction. Also, the possibility to consciously accept mismatching was introduced.

It is worth mentioning some of the relevant changes from the 5<sup>th</sup> iteration (which description can be seen in [AFP11]):

- Removal of the red and blue icons inside the two-dimensional table representing if data was being requested for a specific purpose.
- Introducing color to the circled numbers inside the table, ➤<sup>1</sup>, which represent the data controllers requesting information. Colour was used so to make the connection between the table and the list of service providers in the legend more visible.
- Moving the legend, i.e., the list of data controllers, to the bottom of the table, instead of above.
- Updating the mismatching icon so that it did not look like a logotype.
- Removing the help panel, since it occupied space and eye-tracking data revealed that participants did not read it the help text provided.

The usability tests of the 6<sup>th</sup> iteration cycle (Figure 39) conducted at KAU and CURE revealed that the test participants had in general only few problems with dealing with this prototype. The six participants who filled out the post-test questionnaire at CURE rated their satisfaction with an average of 1.83 (1= very high, 5= very low). All of them stated that they would recommend the tool to their friends.

The usability testing however also revealed some of the remaining usability issues of the dialog that still needed to be addressed. During the usability tests, a cognitive walkthrough method was employed [WRLP94] and eye-tracking data was recorded. The following points describe the relevant results obtained from usability testing at KAU with the help of 10 test participants, along with suggestions for improvement that were included in the interface for the 7<sup>th</sup> cycle.

**Send Data?**

Your data will be sent and used for the following purposes

	Admin	Contact	Feedback	Marketing	Payment
Name - Certified By: Driver's License [Swedish] - S... Inga Vainstein	➤ <sup>1</sup>	➤➤	➤ <sup>1</sup>	➤ <sup>1</sup> ➤➤	-
Cardnumber - Certified By: Visa Credit Card [My private c... 1234 5678 9012 3456	-	-	-	-	➤ <sup>1</sup> <sup>2</sup>
Expirationdate - Certified By: Visa Credit Card [My private c... 2012-01-01	-	-	-	-	➤ <sup>1</sup> <sup>2</sup>
Email: [Empty field]	➤ <sup>1</sup>	➤➤	➤ <sup>1</sup>	➤ <sup>1</sup> ➤➤	-

➤ Data will be sent to:  
<sup>1</sup> eBay Inc. checkout (www.ebay.com, contact@ebay.com) [Privacy Policy](#)  
<sup>2</sup> Visa (www.visa.com, customersupport@visa.com) [Privacy Policy](#)

➤➤ Data will be forwarded to others  
 - Data will not be sent

**Privacy policy matching**

Your [Privacy Settings](#) do not match with <sup>1</sup>'s [Privacy Policy](#).

Found mismatches:

- You do not allow your Name to be used for: Contact, Feedback, Marketing
- You do not allow your Email to be used for: Contact, Feedback, Marketing
- You do not allow your Name to be forwarded to others for: Contact, Marketing
- You do not allow your Email to be forwarded to others for: Contact, Marketing

My current privacy settings:  
 Nearly Anonymous

☐ Accept mismatch  
 for this transaction only




Cancel Send

Figure 39: “Send Data?” dialog: Design of the 6<sup>th</sup> iteration cycle

- Four out of ten test participants at KAU had a hard time noticing quickly and clearly the purposes for which data was being requested, although most of them understood them after a short time of interacting with the dialog. It was suspected that this problem arose due to a lack of visibility on the column headings representing the purposes of data usage, since eye-tracking data suggested that participants did not read or notice the headings for each column of the table. Also some test participants at CURE had problems to directly understand the table and its content. Most of them overcame this comprehension problem after a few moments looking at it. A suggestion was made to add the title “Purposes” above the columns and making the columns’ headings more visible, as well as to provide better help functions.
- Four out of ten participants at KAU expressed their wish to visualize the *mismatches* within the table or interpreted the table as being a representation of their own privacy settings. The purpose of the table, however, is to present a clear and visual-friendly summary of the service provider’s privacy policy. During the most recent tests it was observed that the table can also help users deduce a privacy mismatch as long as they have their privacy settings in mind. However, the bottom panel is meant to give users a more user-friendly and not too alarming visual representation of mismatches by showing a puzzle piece icon. The use of an icon supports the usability heuristic of “recognition rather than recall”, which lets the user visually recognize a mismatch, instead of forcing them to keep their privacy preferences in mind all the time. From the results of a post-questionnaire, seven out of ten said that they understood the purpose of the puzzle-piece icon.
- Eight out of ten participants reported understanding that, at the moment of sending data, only the attributes of each selected credential is sent, and not the whole credential itself. This is an improvement from the tests performed with the design of the 5<sup>th</sup> iteration [AFP11], where participants believed that the whole credential was sent. Curiously enough, no redesign in the 6<sup>th</sup> iteration was made on the visualization or the way participants selected credentials. However, removing the colorful buttons from the table might have had an impact on the way credential selection was perceived (i.e., a less confusing table). Some improvements to the table were suggested, so that users are able to recognize and select credentials in an easier way. For example, having different colors for each row (credential) in order to differentiate them visually, as well as representing credentials with icons that can be easily identified by users. Attributes of the related credentials were also grouped together, so that the attributes for the same credit card would be identify as belonging to the same credential. Eye-tracking data showed that there was a better visual connection made between the colored circled numbers inside the table (e.g., ➤①) and the list representing the service providers, compared to the previous iteration. However, the test at CURE also showed that many test users did not see the table legend at the first glance and did not clearly understand the icons in the table entries. Further improvements have been made in the 7<sup>th</sup> iteration so that the logo of the service provider is shown instead of circled numbers (➤Ex).
- Eye-tracking data revealed that participants failed to read the list of found mismatches, presumably due to too much text. Suggested improvements include rewording the mismatches with simpler text and bolding the attributes so that users get an idea of what is not matching in a quicker way.
- Participants appreciated the possibility to manage privacy settings “on the fly”, although some were confused by the labels of the predefined standard privacy settings (“Nearly anonymous”, “Minimum data” and “Requested data”). It was suggested to simplify the labels to make them more understandable by renaming them to “High privacy”, “Medium privacy” and “Low privacy”.

**Send Data?**


Your data will be sent and used for the following purposes

Attributes	Purposes				
	Administration	Contact	Feedback	Marketing	Payment
<b>Name - Certified By:</b>  Driver's License [Swedish] - S... Inga Valenstein	> Ex	>>	> Ex	> Ex >>	-
<b>Credit Card - Certified By:</b>  Visa Credit Card [My private c...] 1234 5678 9012 3456 Exp: 2012-01-12	-	-	-	-	> V
<b>E-Mail:</b> 	> Ex >>	>>	> Ex	> Ex >>	-

> Data will be sent to:  
 Ex Example.com's store subscription (store.example.com, contact@example.com) [Privacy Policy](#)  
 V Visa (www.visa.com, customersupport@visa.com) [Privacy Policy](#)

>> Data will be forwarded to others  
 - Data will not be sent

**Privacy policy matching**

 Your [Privacy Settings](#) do not match with [Ex's Privacy Policy](#) because,  
 your settings say that you want your:  
 - E-Mail not to be used for Marketing purposes  
 - E-Mail not to be retained for 10 days (settings: 7 days)

My current privacy settings:  
 Medium Privacy Settings  
☐ Accept mismatch  
 for this transaction only

Figure 40: “Send Data?” dialog: Design of the 7<sup>th</sup> iteration cycle

Besides the modifications mentioned above, the additional changes have been implemented in the prototype for the 7<sup>th</sup> iteration cycle (seen in Figure 40):

- Providing tool tips inside to the elements inside the table to provide users with information in the case they try to interact with the table.
- Adding meaningful but simple icons to the credentials to make it easier what type of information the credential represents. For example, a card icon would represent a credit card certified credential, the “@” symbol icon would represent the email uncertified credential.
- Dimming the possibility to accept mismatches if there is no mismatch. In other words, the “Accept mismatch” checkbox becomes inactive if the user’s privacy preferences match the data request from the service provider.
- Help text information is provided to the users when clicking on the context help icons.



# Chapter 5

---

## Conclusions

---

This deliverable presents recent results of PrimeLife Activity 4's work on user-friendly representation of privacy-enhancing identity management concepts, including friendly user interfaces for policy display and administration.

The Privacy-Enhancing Technology Users' Self-Estimation Scale presented in Section 2.1, which we developed in PrimeLife and have consistently applied for post-test interviews, has helped us to better evaluate how users value privacy features as secondary tasks of PrimeLife prototypes.

The question of how to induce the correct mental model of users for novel PET concepts for which no obvious real-world analogies exist, remains as an important challenge for the usability of privacy-enhancing identity management. Our recent experiments with different metaphors for anonymous credentials reconfirmed the difficulties in using analogies when describing this novel technology. In our first rounds of tests the majority of users believed that the anonymous credentials would work in the same fashion as the plastic credentials we compared them to. Interestingly, as we report in Section 2.2.2, our latest test revealed that adding a reference to the main difference between the two types of credentials ("adapted") influences the induced mental model of the users and decreased the error rates of addition by more than 60%.

The final usability evaluation of PrimeLife prototypes (Clique, Duddle, Reputation Management Wiki, Privacy Dashboard, Scramble) and policy interfaces ("Send Data?" dialog), which we presented in Sections 2.3 and 3.2, revealed that evaluated prototypes were well accepted by our test participants, who were able to handle the current versions of the prototypes. However, some minor changes and adoptions were still recommended to improve the usability and workflow of all prototypes. These proposed solutions have already been partly implemented.

An important research result for Activity 4 is also the set of PrimeLife policy icons presented in Section 3.1, which were elaborated and chosen by PrimeLife partner ULD based on intercultural tests performed at Karlstad University and an online survey hosted at CURE. As pointed out above, the next important step to take will be the standardisation of the policy icons, which should also ensure that on a long terms policy icons will be interpreted correctly.



# References

- [AFP11] Angulo, J., Fischer-Hübner, S., Pulls, T. & König, U. To appear in 2011, "HCI for Policy Display and Administration" in PrimeLife - Privacy and Identity Management for Life in Europe, eds. J. Camenisch, S. Fischer-Hübner & K. Rannenberg, Springer, pp. 261
- [BeLe10] Van den Berg, B., Leenes, R. (eds.): Privacy Enabled Communities. Deliverable D1.2.1 of the EC FP7 project PrimeLife.
- [Bic08] Bickerstaff, R.: Towards a Commons Approach to Online Privacy - a "Privacy Commons". Presentation at SCL Information Governance Conference 2008, London, May 2008. <http://www.healthymedia.co.uk/scl-2008-may-governance/pdf/scl-2008-05-privacy-commons-roger-bickerstaff.pdf> (2008). Updated presentation: Towards a Commons Approach to Online Privacy for Social Networking Services - a "Privacy Commons".  
[http://www.ico.gov.uk/upload/documents/pio\\_conference\\_2009/roger\\_bickerstaff\\_birdandbird\\_presentation.pdf](http://www.ico.gov.uk/upload/documents/pio_conference_2009/roger_bickerstaff_birdandbird_presentation.pdf) (2009)
- [BPL11] Bibi van den Berg, Stefanie Pötzsch, Ronald Leenes, Katrin Borcea-Pfitzmann, and Filipe Beato: Privacy in social software. PrimeLife Book
- [C011] Cooper, A.: W3C Privacy Ruleset. <http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html> (2011)
- [CDT09] Center for Democracy & Technology: Privacy Impact. <http://www.cdt.org/content/privacy-impact/> [2009]
- [Cra05] Cranor, L.F.: Privacy Policies and Privacy Preferences. In: Cranor, L.F., Garfinkel, S. (eds.): Security and Usability - Designing Secure Systems that People Can Use. O'Reilly, Sebastopol, pp. 447--471 (2005)
- [D2.3.1] Stefano Paraboschi: Second report on mechanisms, PrimeLife 2010 <http://www.primelife.eu/results/documents>
- [DoBoK10] Dobias, J., Borcea-Pfitzmann, K., Köpsell, S. (eds.): Towards a Privacy-Enhanced Backup and Synchronisation Demonstrator. Heartbeat H1.3.6 of the EC FP7 project PrimeLife,  
[http://www.primelife.eu/images/stories/deliverables/h1.3.6\\_Towards\\_a\\_Privacy-Enhanced\\_Backup\\_and\\_Synchronisation\\_Demonstrator\\_Respecting\\_Lifetime\\_Aspects.pdf](http://www.primelife.eu/images/stories/deliverables/h1.3.6_Towards_a_Privacy-Enhanced_Backup_and_Synchronisation_Demonstrator_Respecting_Lifetime_Aspects.pdf) (2010)
- [EC02/58] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).  
[http://eurlex.europa.eu/pri/en/oj/dat/2002/l\\_2011/l\\_20120020731en00370047.pdf](http://eurlex.europa.eu/pri/en/oj/dat/2002/l_2011/l_20120020731en00370047.pdf) (2002)
- [Eur11] EuroPriSe/ULD: Position paper on certifiability of online behavioural advertising systems according to EuroPriSe - Follow-up, January 2011. <https://www.european-privacy-seal.eu/results/Position-Papers/EuroPriSe%20Follow.pdf> (2011)
- [FiWäZ09] Fischer-Hübner, S., Wästlund, E., Zwingelberg, H. (eds.): UI prototypes: Policy administration and presentation version 1. Deliverable D4.3.1 of the EC FP7 project PrimeLife, [http://www.primelife.eu/images/stories/deliverables/d4.3.1-ui\\_prototypes-policy\\_administration\\_and\\_presentation\\_v1.pdf](http://www.primelife.eu/images/stories/deliverables/d4.3.1-ui_prototypes-policy_administration_and_presentation_v1.pdf) (2009)
- [FiZ10] Fischer-Hübner, S., Zwingelberg, H. (eds.): UI prototypes: Policy administration and presentation version 2. Deliverable D4.3.2 of the EC FP7 project PrimeLife,

- [http://www.primelife.eu/images/stories/deliverables/d4.3.2-policy\\_administration\\_and\\_presentation\\_ui\\_prototypes\\_v2-public.pdf](http://www.primelife.eu/images/stories/deliverables/d4.3.2-policy_administration_and_presentation_ui_prototypes_v2-public.pdf) (2010)
- [GCE06] Gideon, J., Cranor, L., Egelman, S. and Acquisti, A. 2006. "Power strips, prophylactics, and privacy, oh my!" In Proc. SOUPS '06, (2006).
- [GPS09] Gomez, J., Pinnick, T., Soltani, A.: KnowPrivacy, June 1, 2009, [http://www.knowprivacy.org/report/KnowPrivacy\\_Final\\_Report.pdf](http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf) - therein: Policy Coding Methodology: [http://www.knowprivacy.org/policies\\_methodology.html](http://www.knowprivacy.org/policies_methodology.html) (2009)
- [Ha09] Hansen, M.: Putting Privacy Pictograms into Practice - A European Perspective. In: Fischer, S., Maehle, E., Reischuk, R. (eds.): Proceedings of Informatik 2009 - Im Focus das Leben. LNI P-154, pp. 1703--1716. Köllen Verlag, Bonn (2009)
- [Hel09] Helton, A.: Privacy Commons Icon Set. <http://aaronhelton.wordpress.com/2009/02/20/privacy-commons-icon-set/> (2009)
- [HNH11] Holtz, L.-E., Nocun, K., Hansen, M. (eds.): Towards displaying privacy information with icons. Proceedings of IFIP/PrimeLife SummerSchool 2010, Springer Verlag (to appear 2011)
- [Ian10] Ianella, R., Finden, A.: Privacy Awareness: Icons and Expression for Social Networks. 8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods incorporating the 6th International ODRL Workshop, Namur, Belgium. [http://semanticidentity.com/Resources/Entries/2010/7/1\\_Virtual\\_Goods+\\_ODRL\\_Workshop\\_2010\\_files/vg+odrl2010-ws-paper.pdf](http://semanticidentity.com/Resources/Entries/2010/7/1_Virtual_Goods+_ODRL_Workshop_2010_files/vg+odrl2010-ws-paper.pdf) (2010)
- [Joh86] Johnson-Laird, P. N. 1986. Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness. Harvard University Press, Cambridge, MA, USA.
- [Jon95] Jonassen, D.H. 1995. Operationalizing mental models: strategies for assessing mental models to support meaningful learning and design-supportive learning environments. In The first international conference on Computer support for collaborative learning (CSCL '95), John L. Schnase and Edward L. Cunnius (Eds.). L. Erlbaum Associates Inc., Hillsdale, NJ, USA, 182-186.
- [KBCR09] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A "Nutrition Label" for Privacy. In SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security, pages 1–12, New York, NY, USA, 2009. ACM.
- [KPS11] Benjamin Kellermann, Stefanie Pöttsch and Sandra Steinbrecher "Privacy-Respecting Reputation for Wiki Users" accepted for IFIPTM 2011
- [Lev03] Levi, A. 2003. How secure is secure Web browsing?. Commun. ACM 46, 7 (July 2003), p 152.
- [Meh07] Mehldau, M.: Iconset for Data-Privacy Declarations v0.1. <http://www.netzpolitik.org/wp-upload/data-privacy-icons-v01.jpg> (2007) [http://www.primelife.eu/images/stories/deliverables/d1.2.1-10.04.23-privacy\\_enabled\\_communities-public.pdf](http://www.primelife.eu/images/stories/deliverables/d1.2.1-10.04.23-privacy_enabled_communities-public.pdf) (2010)
- [Nie92] Nielsen, J. 1992. Finding usability problems through heuristic evaluation. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (CHI '92), Penny Bauersfeld, John Bennett, and Gene Lynch (Eds.). ACM, New York, NY, USA, 373-380.
- [PFHD+05] J.S. Pettersson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, S. Clauss, T. Krieglstein, and H. Krasemann. Making PRIME Usable. In SOUPS 2005 Symposium on Usable Privacy and Security, Carnegie Mellon University, 2005.
- [Pin11] Pinnick, T.: Privacy Short Notice Design - TRUSTe BLOG. Project web site <http://truste.com/blog>
- [Prim] PrimeLife 2008 - 2010. <http://www.primelife.eu/results/documents>

- [Pri09c] PrimeLife WP4.3. UI Prototypes: Policy Administration and Presentation – Version 1. In Simone Fischer-Hübner, Erik Wästlund, and Harald Zwingelberg, editors, PrimeLife Deliverable D4.3.1. PrimeLife, <http://www.PrimeLife.eu/results/documents>, June 2009.
- [Pri10] Privicons project. <http://privicons.org/projects/icons/> (2010)
- [Pri10] PrimeLife. Scramble! <http://www.primelife.eu/results/opensource/65-scramble>, September 2010
- [Pri10a] PrimeLife WP4.1 HCI Research Report - Version 1, Fischer-Hübner, S., Köffel, C., Wästlund, E., Wolkerstorfer, P., February 2009.
- [Pri10b] PrimeLife WP4.1. High-level Prototypes, C. Graf, P. Wolkerstorfer, E. Wästlund, P. Wolkerstorfer, S. Fischer-Hübner & B. Kellermann, editors. PrimeLife Deliverable D4.1.4. PrimeLife <http://www.primelife.eu/results/documents>, August 2010.
- [Pri10c] PrimeLife. Scramble! <http://www.primelife.eu/results/opensource/65-scramble>, September 2010
- [Pri10d] PrimeLife WP4.3. UI Prototypes: Policy Administration and Presentation – Version 2. In S. Fischer-Hübner and H. Zwingelberg, editors, PrimeLife Deliverable D4.3.2. PrimeLife, <http://www.PrimeLife.eu/results/documents>, June 2010.
- [PriPer] Koeffel, Ch., Waestlund, E., Wolkerstorfer, P., PrimeLife Personas: <http://www.primelife.eu/results/documents>
- [PWG10] Stefanie Pöttsch, Peter Wolkerstorfer, and Cornelia Graf. 2010. Privacy-awareness information for web forums: results from an empirical study. In Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries (NordiCHI '10). ACM, New York, NY, USA, 363-372. DOI=10.1145/1868914.1868957 <http://doi.acm.org/10.1145/1868914.1868957>
- [Ras11] Raskin, A.: Privacy Icons - Making your online privacy rights understandable. Project web site <https://www.drumbeat.org/en-US/projects/privacy-icons/> and <http://www.azarask.in/blog/post/privacy-icons> (2011)
- [Run06] Rundle, M.: International Data Protection and Digital Identity Management Tools. Presentation at IGF 2006, Privacy Workshop I, Athens. <http://identityproject.lse.ac.uk/mary.pdf> (2006)
- [WFH11] Erik Wästlund and Simone Fischer-Hübner. Chapter 12 (The Users' Mental Models on their Comprehension of Anonymous Credentials) in: Privacy and Identity Management for Life. In: Jan Camenisch et al. (ed.) Springer. 229-240, May 2011.
- [WP2/10] Article 29 Data Protection Working Party: Opinion 2/2010 on online behavioural advertising, WP 171. [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf) (2010)
- [WRLP94] Wharton C, Rieman J, Lewis C, Polson P. The cognitive walkthrough method: A practitioner's guide. Usability Inspection Methods 1994:105-40.
- [WT99] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: a Usability Evaluation of PGP 5.0. In SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium, pages 14–14, Berkeley, CA, USA, 1999. USENIX Association.
- [You08] Young, I. 2008. "Mental Models: Aligning Design strategy with human behavior." Rosenfeld Media, New York.

# Appendix A

## Appendix A: PET-USES

### Instructions

This test is designed to measure your experience with the system you've tested today. Your answers will be used to evaluate the system so please answer the questions as truthfully as you can. As the questions are designed to measure various aspects of the systems usability there are no right or wrong answers. Please use the scale below to indicate to what extent you disagree or agree to the statements that follow.

- 1 Strongly disagree
- 2 Disagree
- 3 Neither agree nor disagree
- 4 Agree
- 5 Strongly agree

### General usability

- |   |           |
|---|-----------|
| 1. I found it easy to learn how to use the <i>system</i>                                      | 1 2 3 4 5 |
| 2. I had to learn a lot in order to use the <i>system</i>                                     | 1 2 3 4 5 |
| 3. I keep forgetting how to do things with this <i>system</i>                                 | 1 2 3 4 5 |
| 4. I need a lot of assistance to use this <i>system</i>                                       | 1 2 3 4 5 |
| 5. I find the <i>system</i> interface easy to use   | 1 2 3 4 5 |
| 6. I find the organisation of the <i>system</i> interface understandable                      | 1 2 3 4 5 |
| 7. I get confused by the <i>system</i> interface  | 1 2 3 4 5 |
| 8. I find it very difficult to work with the <i>system</i>                                    | 1 2 3 4 5 |
| 9. I find that the benefits of using the <i>system</i> are bigger then the effort of using it | 1 2 3 4 5 |
| 10. I would like to use this <i>system</i> regularly  | 1 2 3 4 5 |

### Data management

- |  |           |
|--|-----------|
| 11. I get a clear view of my personal <i>data</i> from the system                            | 1 2 3 4 5 |
| 12. I find organising my personal <i>data</i> easy with this system                          | 1 2 3 4 5 |
| 13. I find keeping track of various user names and passwords is easy with this <i>system</i> | 1 2 3 4 5 |

### Credential management

- |  |           |
|--|-----------|
| 14. I find it easy to add personally issued credentials into the <i>system</i> | 1 2 3 4 5 |
|--|-----------|

15. I find it easy to add / import certificates into the <i>system</i>	1 2 3 4 5
16. I find it easy to manage my certificates and credentials	1 2 3 4 5
<b>Privacy Preferences</b>	
17. I find it easy to use settings for how much or how little <i>data</i> to be released	1 2 3 4 5
18. I find that the <i>system</i> helps me understand the effects of different privacy settings	1 2 3 4 5
19. I feel safer knowing that I will be notified if I'm about to release more <i>data</i> than my chosen preference	1 2 3 4 5
<b>Recipient Evaluation</b>	
20. The <i>system</i> makes it easy to decide if it is safe to release my data	1 2 3 4 5
21. I don't understand how the <i>system</i> determines if a data recipient is trustworthy	1 2 3 4 5
22. I feel safer releasing my personal data when the <i>system</i> states it's ok	1 2 3 4 5
<b>Data Release</b>	
23. I know what personal information I'm releasing	1 2 3 4 5
24. I find it easy to decide how much or how little <i>data</i> to release in a given transaction	1 2 3 4 5
25. I get help from the system to understand who will receive my <i>data</i>	1 2 3 4 5
<b>History</b>	
26. I can easily find out who has received my personal <i>data</i> with this <i>system</i>	1 2 3 4 5
27. I get a good view of who knows what about me from this <i>system</i>	1 2 3 4 5
28. I can easily see how much I've used a particular username with this system	1 2 3 4 5

---

*Headings and numerals are mainly for presentational purposes and thus optional during the use of PET-USES. Items 2, 3, 7, 8, and 21 should be reversed before summated.*

# Appendix *B*

---

## Appendix B: Usability Heuristics

---

The used heuristics bases on the Ten Usability Heuristics presented by Nielsen ([http://www.useit.com/papers/heuristic/heuristic\\_list.html](http://www.useit.com/papers/heuristic/heuristic_list.html)).

- **Consistency:** Consistency describes a common design of elements and processes from the users' point of view; all user interface concepts should thus be consistently designed
- **Feedback:** Feedback means that users expect a sufficient system reaction to all of their actions
- **Efficiency:** The user interface must enable the users to carry out their tasks efficiently
- **Flexibility:** The system must allow different users to work differently, or a single user to work differently if he wishes or needs to, in order to accomplish goals
- **Clearly marked exits:** The user must always know how he can leave a specific context, window or display when working with a user interface, and how he can return to his starting position
- **Wording in the users' language:** Wording in the user interface must be known and easily understandable to the user
- **Task orientation:** A user interface shall always be designed to best possibly suit the users' tasks; never shall a user need to adapt to a system
- **Control:** The user must always be in control of the system; the user must never have the feeling of the system controlling him
- **Recovery and forgiveness:** The system must prevent the user from (unknowingly) taking severe actions; the user shall be able to undo changes or actions easily
- **Minimize memory load:** The user shall be able to completely focus on his task, not being troubled with the user interface as such; therefore the user interface must require as little cognitive effort as possible
- **Transparency:** The user must always know what will happen when he takes an action- the user interface must be transparent
- **Aesthetics and emotional effect:** Everything has an emotional effect; if a user interface has an inappropriate emotional effect, it will interfere with the users' tasks



