Privacy and Identity Management in Europe for Life

# HCI Research Report - Version 1


| | |
|---|---|
| Editors: | Simone Fischer-Hübner (KAU) |
| | Christina Köffel (CURE) |
| | Erik Wästlund (KAU) |
| | Peter Wolkerstorfer (CURE) |
| Reviewers: | Jan Camenisch (IBM) |
| | Sandra Steinbrecher (TUD) |



| | |
|---|---|
| Identifier: | D4.1.1 |
| Type: | Deliverable |
| Version: | 1.0 |
| Class: | Public |
| Date: | February 27, 2009 |



**Abstract**

One of the core activities in the *PrimeLife* project is the design and implementation of privacy aware applications that are usable. Therefore it is the main objective of Activity 4 to assure the usability of those applications and advance the research in this area. The First HCI Research Report presents the main research results of the HCI activity within the first year of *PrimeLife*. The HCI Research Report V1 presents work in progress and will be updated and complemented by a second version, the Final HCI Research Report (D4.1.5), which will be published at the end of the *PrimeLife* project.



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


# Members of the PrimeLife Consortium

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

# List of Contributors

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

| **Chapter** | **Author(s)** |
|---|---|
| Chapter 1, Introduction | Simone Fischer-Hübner (KAU)<br>Christina Köffel (CURE)<br>Peter Wolkerstorfer (CURE) |
| Chapter 2, Methods | Christina Köffel (CURE)<br>Maren Raguse (ULD)<br>Erik Wästlund (KAU)<br>Peter Wolkerstorfer (CURE) |
| Chapter 3, UI Representation of Privacy-enhancing Identity Management Concepts | Simone Fischer-Hübner (KAU)<br>Christina Köffel (CURE)<br>Erik Wästlund (KAU)<br>Peter Wolkerstorfer (CURE)<br>(Jan Camenisch (IBM) and Ronald Leenes (TILT) contributed to the Section on "Credential Selection Paradigms") |
| Chapter 4, HCI for Trust and Assurance Evaluation | Simone Fischer-Hübner (KAU) |
| Chapter 5, User Friendly Policy Management and Presentation | Mike Bergmann (TUD) |
| Chapter 6, Conclusions and Outlook | Simone Fischer-Hübner (KAU)<br>Christina Köffel (CURE)<br>Erik Wästlund (KAU)<br>Peter Wolkerstorfer (CURE) |

| Chapter | Author(s) |
|---|---|
| | Besides, the members of the *PrimeLife* HCI activity, namely Mike Bergmann (TUD), Simone Fischer-Hübner (KAU), Hans Hedbom (KAU), Christina Köffel (CURE), John Sören Pettersson (KAU), Maren Raguse (ULD), Erik Wästlund (KAU), Peter Wolkerstorfer (CURE), as well as other *PrimeLife* members, particularly Benjamin Kellermann (TUD) and Gregory Neven (IBM), contributed to the discussion of mock-up proposals that are presented in Chapters 3 to 5. John Sören Pettersson also contributed to the development of the Trust Evaluation mock-ups presented in Chapter 4. Maria Lindström (KAU) contributed to the usability tests of the Trust Evaluation mock-ups that were performed at KAU. |

# Executive Summary

*PrimeLife* has the vision of bringing sustainable and user-controlled Privacy and Identity Management (IDM) to future networks and services. User-controlled Privacy and Identity Management implies that users can make informed choices about the releases of personal data, the selections of credentials for proving personal properties, their privacy and about trust policy settings. For enabling users to make well-informed decisions, user interfaces (UIs) are needed that inform them about the trustworthiness and the privacy policies of their communication partners as well as the implications of personal data releases. These user interfaces should be informative while not being perceived as intrusive, intuitive and well understandable, legally compliant and trustworthy. The challenges of researching and developing such user interfaces are addressed by *PrimeLife* Activity 4 (HCI).

The first Chapter of the present HCI Research Report V1 introduces the background and objectives of HCI research within *PrimeLife*, related work and the structure of this deliverable. The remaining Chapters present the HCI research results of *PrimeLife* Activity 4 and its Work Packages within the first project year of the *PrimeLife* project.

Work Package 4.1 (UI Representation of Privacy-Enhancing Identity Management Concepts) has in the first project year investigated suitable and novel methodologies and success criteria for evaluating privacy-enhancing technologies (PETs) that have been applied to the evaluation of the UIs developed by Activity 4. These include personas Walkthroughs based on the personas developed within *PrimeLife*, the CURE virtual usability laboratory for asynchronous online tests, as well as PET-USES (the Privacy-Enhancing Technology Users' Self-Estimation Scale) which is a modified and extended version of SUS (System Usability Scale) for measuring the usability of privacy related UI aspects. The results of WP4.1's work on methodology and success factors is documented in chapter 2 (Methods) and section 3.2, which also presents the CURE virtual usability laboratory.

Furthermore, Work Package 4.1 has conducted usability tests of prototypes to detect usability issues of privacy-enhancing IDM technologies that need to be addressed and has researched mental models and metaphors for PET concepts. As *PrimeLife* is building upon results of the previous FP6 project *PRIME*, laboratory usability tests of the latest *PRIME* integrated prototype V3x were performed. The results obtained through the evaluation have an impact on HCI research work within *PrimeLife* and are therefore reported in Chapter 3 of this Research Report. While the results of the evaluation revealed several usability issues, such as inconsistencies, problems of clarity, information overloads, they also showed that users appreciate the *PRIME* functionality and specifically end user transparency tools such as the *PRIME* data track. Important is also to mention that some usability issues such as unclear user warnings led to a lower degree of trust in the system.

Chapter 3 also reports about Work Package 4.1's work on mental models of credential selection and anonymous credential selection mock-ups. This research work is especially challenging as there are no direct analogies for anonymous credentials in the real world. Previous mock-up proposals for anonymous credential selection developed in *PRIME* revealed that end users did not understand the data minimisation property of anonymous credentials and thought that proofs of certain attributes of a credential would reveal the complete credential including all its attributes. As reported in Chapter 3, current research in Work Package 4.1 uses the paradigm of derived virtual cards containing only a selection of attributes or characteristics of attributes to illustrate the fact that only those data of the virtual card are revealed.

Chapter 4 presents on the research results of Work Package 4.2 (HCI for Trust and Assurance Evaluation), which has in the first project year mainly conducted research on a usable trust evaluation function, which allows end users to evaluate the trustworthiness of communication partners in terms of privacy and business reliability. This trust evaluation function evaluates the degree of trustworthiness of a side based on information provided by trustworthy parties, such as privacy seals awarded by data protection commissioners, or information whether a side is blacklisted by consumer organisation or mentioned on privacy alert lists, as well as dynamically generated assurance claims about the privacy functionality of the communication partner's system. User interface mock-ups that we developed for such a trust evaluation function try to address several challenges, such as the challenge of illustrating parameters with different semantics and scopes, using intuitive icons, and the challenge of informing the users while avoiding extensive warnings. In the mock-ups, trust evaluation results are presented on multiple layers: An overall evaluation result on the top layer is presented in situations when users are requested to disclose personal data. Users who are interested in more evaluation details can view the evaluation results of the different parameters (privacy seals, blacklists, privacy alert lists, *PrimeLife* functionality) on the next layer, which can in turn be expanded for further details. First usability tests in Ozlab at Karlstad University revealed that users appreciated such the functionality and well understood the overall trust evaluation results presented on top level. The more detailed trust evaluation results on the second layer were, however the harder to understand for some test users. Further research needs to be done for finding particular suitable icons and for finding suitable illustrations for the situations that there is no information about certain parameters (e.g. the side has no privacy seal and is not blacklisted).

Chapter 5 presents research results by Work Package 4.3 (Privacy Policy Management and Display). It particularly defines a set of three predefined privacy preferences (so-called PrivPrefs). The first PrivPref defines the preference of releasing no personally-identifiable data at all, i.e. for remaining anonymous. The second PrivPref defines the preference of releasing only minimal data needed for a certain purpose while the third PrivPref allows revealing more data than needed (usually in return for certain benefits, e.g. to release an e-mail address for receiving special offers as a bonus customer). For each combination of communication partner and purpose, one of these privacy preference types for personal data releases to this specific communication partner for this specific purpose can be assigned. If for a combination of communication partner and purpose no PrivPref type has been assigned, the preference of no personally-identifiable data is taken by default. However, this preference settings can be adapted "on the fly". If for example a

user agrees to release data needed for a service (e.g. reveal his address to a delivery service for the delivery of purchased items), the user can at the same time change the PrivPref type for the respective service provider and purpose from "No personally-identifiable data" to "only minimal data". This approach of offering pre-defined preferences, from which a user can choose "on-the fly", should simplify privacy policy management for the users. Users can also be warned about excessive data requests if the PrivPref type "only minimal data" has been chosen.

Moreover, Chapter 5 presents some novel approaches of dynamic presentation of a services side's privacy policy and its (mis-)matches with a user's chosen PrivPrefs. With this dynamic presentation approach, information about (top-layer) short policy notices and their correspondence with the user's preferences appears visibly in the moment when a user is hovering the mouse over a form, where he has to fill in personal data. A more detailed condensed or full privacy notice can be viewed with additional mouse clicks. The sudden occurrence of control elements should help to attract the user's attention. First pilot tests performed with CURE's virtual usability laboratory also revealed that users recognise such dynamic privacy policy display interfaces much easier.

The final chapter provides main conclusions as well as an outlook to future research activities within *PrimeLife* Activity 4.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 *PrimeLife* and its HCI Research

The *PrimeLife* project has the vision of bringing sustainable Privacy and Identity Management (IDM) to future networks and services, and is therefore contributing with research and development of configurable and scalable privacy-enhancing IDM solutions, with a special focus on emerging and established Internet applications and services, such as virtual communities. According to Pfitzmann and Hansen, IDM means managing various partial identities (i.e. set of attributes, usually denoted by pseudonyms) of a person, i.e. the administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role [PH01]. Privacy-enhancing IDM is also sufficiently preserving unlinkability (as seen by an attacker) between the partial identities of an individual person required by applications [PH01]. The *PRIME* project has already demonstrated the feasibility of privacy-enhancing IDM systems providing maximum privacy by integrating state-of-the art and novel privacy-enhancing and transparency enhancing technologies. *PrimeLife* builds upon and advances the *PRIME* project approach. In particular, it provides privacy features by deploying the following privacy-enhancing technologies (PETs):

- **Data minimisation** with the help of anonymous communication technologies, anonymous credentials and privacy-enabling authorisation schemes.
- **Assurance (Trust) & Life Cycle Management** with the help of assurance control, privacy and trust policy negotiation and enforcement, obligation management, and multilaterally secure reputation systems, which can specifically help to evaluate and establish trust in other peers.
- **Transparency** with the help of end user tools that keep track of all data releases by a user, allows the end user to access his data stored by others online, and tools that inform him about the implications of future data releases.

Privacy-enhancing IDM will however only be successful if its technologies can be easily handled, are trusted and accepted, legally compliant and employed by the end users.

Most of these *PrimeLife* technologies listed above require end user interfaces, which enable the users to make informed choices. These include choices concerning the selection of appropriate (anonymous) credentials for proving personal properties, the release of personal data items, the selection and adoption of privacy and trust policies. For enabling well-informed decisions, the user interfaces have to present information about the trustworthiness of communication partners as well as information about privacy implications of those choices in terms of the linkability of the user's partial identities and of their communication partners' data handling policies. This information about choices and their implications must be well understandable, noticeable and complying with legal requirements, but should at the same time not be perceived as too interfering and disturbing. Also actions needed for performing choices should be easy to handle.

For this reason, the research and development of user interfaces for *PrimeLife* technologies that are intuitive, user-friendly and compliant with legal and social requirements play a key role. Privacy-enhancing IDM for virtual community applications will have to take specific legal, social and technical aspects into account, which will have an influence on the HCI (Human Computer Interaction) solutions to be developed in *PrimeLife* Activity 4 (HCI).

Some of the HCI Challenges described above, including for instance the challenge how to map legal privacy requirements into HCI constructs, have already been at least partially addressed within the *PRIME* project and other related projects. The HCI research within *PrimeLife* aims particularly at addressing the following research challenges that we think specifically need further attention:

- Privacy-enhancing technologies (PETs) are based on complex technical concepts or constructs such as pseudonyms, unlinkability and anonymous credentials that are unfamiliar to many end users and often do not fit to their mental picture of what belongs to an electronic identity and how it can be technically protected. How can a notion about electronic identity be illustrated to the user for estimating the risk of being identified across different interactions with one or several communication partners? Within the *PrimeLife* project, these challenges are researched by Work Package 4.1 (*Representation of Privacy-enhancing IDM Concepts*). In the first project year, Work Package 4.1's research work for addressing these problems has put an emphasis on researching user-friendly ways for presenting anonymous credential schemes (see Chapter 3).

- How can the user interfaces mediate reliable trust in *PrimeLife* technology and communication partners to end users? For addressing this problem, we have within Work Package 4.2 (*Trust and Assurance HCI*) in the first project year conducted research on the design of a user-friendly trust evaluation function which can convey information, which is stated or certified by third (trustworthy) parties, to end users about the level of trustworthiness of communication partners (see Chapter 4). User-friendly transparency tools are also means for enhancing the users' trust in *PrimeLife* technologies, which we will further research in the next two project years. These will also include transparency tools for social community users.

- How can privacy and trust policy definitions, administration and negotiations for end users and system administrators be simplified by appropriate means for pol-

icy presentation, presettings and automation in a way compliant with European privacy legislation? These challenges are addressed by Work Package 4.3 (*Interfaces for Policy Display and Administration*), which has in the first project year researched novel concepts for a simplified management of privacy preferences and user-friendly display of data handling policies of services sides including information about how far they match with the user's privacy preferences (see Chapter 5). In the next two project years also new forms of displaying policy-related information during the process of policy negotiation between individual virtual community users will be researched.

Besides, a special focus of the research work of Work Package 4.1 has also been on the research and development of novel methodologies for evaluating HCI solutions for PETs that can be used within *PrimeLife*, because existent methods, such as available system usability scales and questionnaires for measuring user experiences and usability of various HCI aspects, do not address PET related issues.

## 1.2 Aims and Scope of the HCI Research Report

The objective of this deliverable D4.1.1 (HCI Research Report V1) edited by *PrimeLife* Work Package 4.1 is to present the main research results of *PrimeLife*'s HCI activity within the first project year. It includes also results of usability evaluations of *PRIME* technology, which were conducted at the beginning of the first year, as those results have an important influence on our subsequent HCI research and development work. Nevertheless, a clear focus of this report is on HCI research conducted within the first project year. This means that other work conducted within the HCI activity that is not directly related to research results, such as the evaluation of the *PrimeLife* website or programming development work, are not reported here.

The HCI Research Report V1 presents work in progress and will be updated and complemented by a second version, the Final HCI Research Report (D4.1.5), which will be published at the end of the *PrimeLife* project.

The HCI Research Report's target audience comprises all other *PrimeLife* partners, because the HCI work in *PrimeLife* is also related to all other *PrimeLife* activities, as well as the HCI and PET research and development community outside of *PrimeLife*.

Within this document, the test participants and users of the developed prototypes will be referred to as "he" (male form) only for reasons of simplicity, without any intend to exclude females.

## 1.3 Related work

While research on usable security and privacy has received more attention in the recent years, most research work performed and published in this area addresses specific problems or provides general guidelines on usable privacy (see for instance [Yee02], [JEL03], [Gar05], [HS07]). We will reference to some of these works in the subsequent chapters of this deliverable.

There is however not much published research work yet that addresses a wider scope of usability aspects of PETs or more specifically of privacy-enhancing IDM. Some relevant

related work on the usability of PETs has been conducted and reported by the EU FP5 project PISA, which however had its emphasis on mapping legal privacy principles into HCI requirements and possible solutions [PKHvB03]. Also the HCI activity of the *PRIME* project has addressed similar research questions, and has built upon and extended the research work of the PISA project. Parts of the *PRIME* HCI research results have been presented in the *PRIME* HCI Guidance deliverable D6.1.f [Pet08] and have been summarised in [FHPB+09]. In contrast to this HCI research report, the primary purpose of the *PRIME* HCI Guidance Deliverable was not to serve as a research report but rather to define HCI requirements for the design and evaluation of privacy-enhancing IDM. Even though *PrimeLife* is partially building on the *PRIME* HCI research results, it is also addressing HCI challenges that have not been addressed or solved to a satisfactory degree or that arise specifically for virtual community applications.

Further related work taking a wider perspective on privacy and HCI is provided by Iachello and Hong [IH07], which outlines current approaches, results and trends of PET-related HCI research and identifies open research issues. Their report is however not specifically addressing HCI for privacy-enhancing IDM. Dhamija and Dusseault discuss in a recent publication flaws of IDM posing HCI and security challenges and providing some recommendations how to address them [DD08]. However, in contrast to this HCI research report, their work has not a specific focus on HCI of privacy-enhancing IDM either.

## 1.4 Structure of this Document

The remainder of this document is structured into the following chapters, which present the main activities and research results in the first project year of the *PrimeLife* Work Packages within Activity 4 as already briefly outlined above in Section 1.1:

- Chapter 2 (*Methods*) describes the evaluation methods and success criteria that were employed and also partly developed by *PrimeLife* Work Package 4.1.
- Chapter 3 (*UI Representation of Privacy-enhancing Identity Management Concepts*) summarises additional main research results of *PrimeLife* Work Package 4.1. These comprise results from usability tests including conclusions drawn from those tests which have an impact on our HCI research, as well as first results on research on mental models and mock-ups, where a special focus has been on anonymous credential selection.
- Chapter 4 (*HCI for Trust and Assurance Evaluation*) reports about our research conducted by Work Package 4.2 on mediating reliable trust to end users with the help of a usable trust evaluation function, which represents the trustworthiness of communication partners in terms of privacy and business reliability.
- Chapter 5 (*User-friendly Policy Management and Presentation*) is presenting novel means for configuring the user's privacy preferences "on the fly" and for presenting data handling policies and their (mis-)matches with the user's preferences, and thereby refers to the research by Work Package 4.3.
- Finally, Chapter 6 is providing conclusions and an outlook.

# Chapter 2

# Methods

A crucial point in any IT (information technology) system is the analysis and evaluation if the design of the application is **usable**, offers the users **additional value** and **supports** them in their daily work. Especially when dealing with PETs (privacy-enhancing technologies) there is a great demand for highly efficient and easy to use products. PET technologies deal with personal and sensitive data, making it utterly important for the user to be understandable, efficient and not misleading.

Therefore it is of great importance that the user interface (UI) of the *PrimeLife* application leads to a highly effective and sufficient **user experience**. To reach this goal it is necessary to set up a validation plan that covers all different aspects of the *PrimeLife* system.

The following sections provide an outline of the methods employed for the validation of the *PrimeLife* demonstrators and applications, as well as legal aspects in the development of these solutions. Furthermore the PET-USES, a new approach towards a questionnaire-based evaluation of PETs will be introduced.

## 2.1 Objectives of the Evaluations

As mentioned previously, it is an objective of *PrimeLife* to create efficient and easy to use products. This is especially regarded in Activity 4. Therefore it is the main goal of Work Package 4.1 (which is part of Activity 4) to create usable and understandable PET solutions.

The success is defined by measures as indicated in Table 2 (for details on the measures refer to Appendix D "Description of Work" of the *PrimeLife* project).

| Measure | Means |
|---|---|
| 80% of the users are able to conduct at least 80% of a given privacy-task-set without intervention | Laboratory usability test; Questionnaire |
| 80% user satisfaction with ease of use | SUS (system usability scale), Questionnaire |

| Measure | Means |
|---|---|
| 80% user satisfaction with privacy results | PET-USES |
| 20% reduction of privacy-setting faults | Laboratory usability test, Logfile analysis |
| 50% improvement in the accuracy of privacy settings | Laboratory usability test, Logfile analysis |
| 95% usage by users designated by the pilot site demonstrators | Logfile analysis |
| Ability to successfully conduct privacy tasks increased on average by 50% | Laboratory usability test, Questionnaire, Logfile analysis |
| 50% improvement in the understanding of privacy settings | Laboratory usability test |
| Ability to adopt correct privacy settings increased by 20% | Laboratory usability test |
| Demonstrable UI mock-ups & prototypes | Iterative Design |
| Fully documented user validation findings published | Documentation |
| Design patterns covering 100% of PET scenarios of *PrimeLife* | Documentation |

Table 2: Measures of success as defined in Appendix D of the *PrimeLife* Project.

## 2.2 Introduction to Methods

In accordance to the success criteria as introduced in section 2.1, the *PrimeLife* user interfaces will be fully tested and validated within Activity 4. The subsequential paragraphs will present the methods employed for testing.

### 2.2.1 End-user testing

One of the main goals is the development of a usable application. Therefore it is crucial that the user interface of the *PrimeLife* application leads to a good user experience. To ensure this goal, a combination of different methods will be used to gather information from different perspectives. The end-user testing identifies (for a more detailed version of the *PrimeLife* evaluation plan please refer to [CKU08]):

- Objectives of the tests
- The testing procedures to be undertaken (mix of methods)

The testing includes "informal" and "formal" methods. In both cases the results are summarized in test reports that form the basis of the final User Validation Analysis Report (D 6.1), containing also suggestions how the applications can be improved, respectively which necessary corrective actions should be undertaken to improve the user experience of the system.

In the following paragraphs the set of different methods being used are described.

### 2.2.2 HCI Expert Evaluations of UIs

Before laboratory tests are undertaken, expert evaluations will be conducted in order to detect the most prominent usability problems, which could lower the acceptance of the *PrimeLife* PETs. The evaluations will produce qualitative results and contribute to the general improvement of the usability of the UIs in *PrimeLife*. The main method being used is the heuristic evaluation. The resulting input to the project will be in form of a list of identified problems with comments including redesign suggestions. The heuristic evaluations will be conducted in fine granular iterative steps during the development of the UIs in *PrimeLife*.

### 2.2.3 Personas

In the following paragraphs the persona-method will be introduced. Furthermore we will reason on the use of personas in *PrimeLife* and provide a brief description.

In the task description of Task 4.1.1 (page 81, Annex I "Description of work") we promise that:

> The results of this task feed directly into the other tasks in this Work Package and **ensure a strong focus on the user** throughout the project.

To achieve the goal of "a strong focus on the user throughout the project" we have decided to use the personas method.

Alan Cooper - "inventor" of the personas method describes it like this:

> "Personas are not real people, but they represent them throughout the design process. They are hypothetical archetypes of actual users. Although they are imaginary, they are defined with significant rigour and precision." [Coo99]

In general personas show the scope and nature of the design problem. Until "the user" is precisely defined, we can always imagine that we ourselves are the users [PA06]. We have different pictures in mind (as shown in Figure 1) which hinder fluent communication.

Personas as communication tool allow defining which users we are building for and synchronize (see Figure 2) the pictures in our minds.

A lot of companies (Microsoft [PG03], Ford, Chrysler, Sovereign Bank, Amazon, Best Buy, Staples, FedEx, UPS, IBM, SAP, SONY, Razorfish, Pfaltzgraff, Yahoo! Media, Electrolux, Cisco [NIA07]) use personas successfully because of their advantages - which are:

1. Support having the **same picture** of our end-users in mind for everybody in the project; hence reduce communication-complexity which makes communication easier and more fluent (this again saves time explaining "the user" every time he appears in a communication process).
2. Bias the minds of everybody in the project toward **user-centred thinking**. This gives the otherwise "technical touch" of R&D projects a humane touch and brings things to live in a natural way (as human minds deal great with other persons - but human minds have a hard time when dealing with abstract big bunches of data) - personas make use of the "Emotional Mind" of people [ST05].

**Figure 1**: We have different pictures in mind which hinder fluent communication.

**Figure 2**: Personas as communication tool allow defining which users we are building for and synchronize the pictures in our minds.

3. Be an **evaluation tool** as walkthroughs can be conducted with personas (which is very handy to judge design alternatives).
4. **Leave** the world of **possibility thinking** as you are very unlikely to fall back to "the user".
5. They can **shorten feature debates** which saves time.
6. A tool to help the whole project team **focus on the needs** of our target **users** instead of using a different ad hoc "the user" definition which comes to mind at a point in time (Humans have just one locus of attention. It lies in the nature of R&D that the developers' locus of attention is focused on the technical issues and not the real end-users. Therefore there is a need for methods solving this missing focus on the end-user. Personas are one way to do it.).
7. Personas are unobtrusive - they do not modify any existing processes and unfold their power subtly in the minds of people; they make thinking about "the user" **more convenient**.
8. Unlike bunches of data personas support **informed design** (you can design UIs

for persons - not for data representations).

9. According to Cooper the design process becomes **"enlightened"**.

More information on personas and a detailed description of the *PrimeLife* personas can be found in Appendix B.

### 2.2.4 Personas Walkthrough

In persona walkthroughs the *PrimeLife* personas are used for an early expert-based evaluation using the cognitive walkthrough method [PA06]. Either one expert or a group of experts steps through a system according to pre-defined context scenarios.

The evaluators imagine themselves to be the personas and the scenarios are created from the personas' perspective. The single tasks of the scenarios represent the persona's typical interaction with the interface and are selected according to the personas' attributes. Therefore the evaluator is able to see the system through the eyes of the user. In this case the user is not only one possible and loosely defined person, but resembles a well-defined target group of the system. Hence, a developed interface can be evaluated from the point of view of all user groups, with a potential concentration on the major target customers.

Persona walkthroughs can be conducted in three different steps. Either they are used for a rapid evaluation of a system, which can take about one to two hours, or they can be used for a more formal review with more detailed modelled tasks. Another possibility is to use persona walkthroughs as a part of larger design efforts.

Employing persona walkthroughs, user-typical design issues can be detected early in the design process. Furthermore also the entire user experience and learnability of a system can be investigated. The outputs of the persona based cognitive walkthrough are usability issues, user experience flaws and concerns, but also detailed suggestions for improvement of the system.

### 2.2.5 Heuristic Evaluations

Expert-based evaluations are conducted using heuristics, which are established usability principles. The following heuristics are employed for evaluating the *PrimeLife* applications:

- **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 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 enabled to focus totally 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, therfore 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 user tasks.

In addition to the principles we also obey the following concepts:

- **Hick's Law:** Model to predict selection times (1 out of n selections).
- **Fitt's Law:** Model of human psychomotor behaviour which enables the prediction of human movement times.
- **Affordance:** An object's sensory characteristics which allows users to imply its functionality and/or usage.
- **Information scent:** A theory on user navigation lead by semantics.
- **Modes:** A state of an application where the application behaves different.
- **Flow:** A mental state where task and users capabilities match.
- **Gestalt:** A theory of mind and brain that proposes that the operational principle of the brain is holistic, parallel, and analog, with self-organizing tendencies; or, that the whole is different than the sum of its parts[1].

### 2.2.6 Logfile Analysis

The *PrimeLife* application will have an inherent amount of logging for audit trail purposes, which will identify knowledge captured or accessed, user, time, date and situation-dependent information such as IP address, origin (country, website), operating system or browser (in case of websites). Logfile analysis can be conducted on operational systems as well as prototypes and will be applied depending on the state of the software available.

[1] `http://en.wikipedia.org/wiki/Gestalt_psychology`

Therefore knowledge derived from logfile analysis can be used to trace the users' actions while using the system in order to detect behavioural patterns in the user's actions.

The trial participants will be informed that their actions with the *PrimeLife* application will get a time stamp and will be saved. They will also be assured that the data will be treated anonymously and that it will not be handed to third parties who are not directly involved with the project. These logfiles will be analysed and used as additional input for the planning of the final focus groups. Example analyses include seeing how long users took to find what they wanted, how many steps they had to take, etc.

### 2.2.7 Laboratory Usability Tests

The goal of laboratory usability tests is the measurement of the applications' usability in terms of task efficiency and user satisfaction. By conducting these formal tests usability problems as well as room for improvement of the *PrimeLife* system will be identified. The test will be conducted with 16 participants from the user group, 8 for each demonstrator. The main objectives of the test will focus on the question if the proposed privacy impact, interface design and interaction design fits the user's needs. To cover these issues the test users will be confronted with typical tasks and will be observed using usability lab equipment. Variables such as the time to complete the task, occurring interaction problems and errors will be monitored (for each concrete test a test-plan will be developed). To test the subjective expectation and satisfaction the users will have to answer a set of questions and fill in a questionnaire before and after the test. The results of the user tests will be the basis for recommendation of system improvements.

In addition to the observations, analysis of the privacy-related settings will be done after the tasks in order to be able to measure the privacy impact of the solutions.

### 2.2.8 KLM-GOMS

The Keystroke Level Model GOMS (KLM-GOMS) modelling technique simplifies estimation of software usage times for systems with GUIs (graphical user interfaces) [CMN80]. The Goals, Operators, Methods and Selection rules (GOMS) family of techniques for modelling human performance have proved to be helpful in estimation of times required to accomplish goals on computer systems. In *PrimeLife* KLM-GOMS will be used to compare different designs in terms of efficiency.

### 2.2.9 SUS - System Usability Scale

Brooke, the creator of the system usability scale, states that usability does not exist in any absolute sense; it can only be defined with reference to particular contexts. This, in turn, means that there are no absolute measures of usability, since, if the usability of an artefact is defined by the context in which that artefact is used, measures of usability must of necessity be defined by that context too. Despite this, there is a need for broad general measures, which can be used to compare usability across a range of contexts. In addition, there is a need for efficient methods to allow low cost assessments of usability in industrial systems evaluation [Bro96].

In *PrimeLife* SUS will be used to monitor the overall progress of usability during the project. This allows capturing the "big picture" of the status quo of usability and making different versions comparable. SUS therefore allows us to quality-control the usability.

### 2.2.10 Focus Groups

Focus groups [Kru88] are a technique that helps to assess the user's experience with a product. In a focus group, six to nine users are brought together to discuss issues and concerns about the features of the examined product. The group typically lasts about two hours and is run by a moderator who maintains the group's focus. Focus groups often bring out users' spontaneous reactions and ideas and let the moderator observe some group dynamics and organizational issues. Focus groups assess what users think about a specific product. Therefore this method is a supplement to actual user tests.

The main purpose of the *PrimeLife* focus groups will be:

1. Elicit mental models of privacy;
2. Gather knowledge about the acceptance of *PrimeLife* applications; and
3. Support the creation of PET-USES (see description in Section 2.4).

The focus groups will be conducted for eliciting the mental models of the users:

- Discussion of typical usage situations and of social or psychological problems;
- Discussion of the systems' utility;
- Discussion of privacy problems; and
- Discussion of the *PrimeLife* applications' interface usability;

Demonstrations for a focus group of yet non-existing products can be made by oral presentation, tests, presentations, UI animations, and demos of interactive mock-ups if no working prototype is available.

### 2.2.11 Questionnaires

A complement to focus groups are questionnaires handed out to a large group of people gathered in a lecture hall or community hall. Demonstrations by UI animations make the set-up possible to repeat. They can also be conducted in computer halls to collect answers in digital format which is also possible in the case of online questionnaires. Questionnaires make it possible to divide the populations in subgroups such as different age groups. The perception of potential user groups can thus be assessed (cf. how this was done in an intercultural study of the TownMap metaphor in the *PRIME* project [BRP05, Pet08]).

The users will be asked about UI animations. UI animations cannot capture usability problems but differences in perceptions of problems, solutions, and UI designs can be captured (the referred intercultural study revealed an age difference but no cultural difference).

## 2.3 Legal Analysis of UIs

To ensure legal compliance of the UI mock-up and prototype development carried out in Work Package 4.1 a legal evaluation and guidance of the development process will be conducted by ULD throughout the entire development process. The guidance aims to ensure all relevant legal requirements are considered and implemented as features of the UIs.

### 2.3.1 Evaluation Methodology

ULD will identify required features of the UI and analyse their appropriate implementation by applying criteria derived from three existing methods for a privacy compliance assessment of products or processes. Good practice, certification schemes and standards regarding information security are well established (e.g. ISO 15408, ISO 27001, ISO TR 13335, and ISO 17799/27002).

Approaches focusing on privacy certification and good practice exist too and will be applied by ULD for the legal evaluation and guidance. Standardisation on a European level is led by the European Committee for Standardization (CEN). Two CEN Workshop Agreements (CWAs) deal with criteria for data protection and privacy practices. CWAs 15499-1 and -2 describe a Personal Data Protection Audit Framework.

A second process related approach - the Privacy Impact Assessment (PIA) - is widely established in Canada, the United States, Australia and the United Kingdom. The British Information Commissioner's Office released a handbook presenting criteria for an analysis of compliance with eight basic data protection and privacy principles transposing Directive 1995/46/EC and therein regulated principles.

Furthermore, criteria developed within the research project EuroPriSe will be applied. EuroPriSe is introducing a European Privacy Seal for IT products and IT-based services. Criteria to assess privacy compliance are derived from Directives 1995/46/EC and 2002/58/EC.

All of the described approaches apply the same methodology. By means of a set of questions criteria for legal compliance are analysed. These criteria are derived either directly from the European privacy directives or from the national Act incorporating the EU directives into national laws. While a PIA's perspective is ex ante, EuroPriSe and the Personal Data Protection Audit Framework originally apply an ex post perspective. For the work on UI in Work Package 4.1 all of the criteria will be applied already at the design stage, so from an ex ante perspective.

### 2.3.2 Expected Results

Applying these criteria during the development process will identify gaps and non-compliance issues as well as design requirements which need to be addressed.

## 2.4 PET-USES

PET-USES [The Privacy-Enhancing Technology Users' Self-Estimation Scale] is a questionnaire that lets users evaluate PET-UIs. The PET-USES includes one part measuring

overall usability and one part measuring PET-aspects. An important feature of the measurement of PET-aspects is that the questionnaire is modular insofar that it is possible to include or exclude scales measuring specific aspects based on the tasks and features being tested. Thus, the PET-usability scales have a dual purpose in that it both evaluates software's general usability and that it evaluates the extent to which the software clarifies privacy related learning issues for the user (version 1.0 of the PET-USES questionnaire is included in appendix A). Although there are a number of questionnaires measuring user experience and usability of various HCI (human-computer interaction) aspects of both software and websites [Bro96, TS04] none include PET related issues.

The reason for developing and using PET-USES is to be able to measure the perceived usability of the UIs being developed both during single user trails and during large group walkthroughs of screen recordings.

The PET-USES questionnaire is based on the ISO 9241 general standard of usability (ISO, 1998) as well as the more domain specific HCI guidelines derived from the *PRIME* integrated IDM prototype [Pet08]. The former defines usability as the "extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction" whereas the latter promotes the four categories comprehension (to understand or know), consciousness (be aware or informed), control (to manipulate or be empowered) and consent (to agree).

Although the two views might seem divergent at first they can readily be combined within the structure of usability testing proposed by Hornbæk [Hor06]. Based on a review of 180 studies, published in core HCI journals and proceedings, he argues for a change in terminology to better encompass what is actually being measured.

Taken together then, possible constructs of interest for the PET-USES questionnaire can be placed within the framework displayed in Table 3.

| Hornbæk | ISO 9241 | HCI Guidelines | Other measures and concepts of usability |
|---|---|---|---|
| Outcomes | Effectiveness | Consent (agree)<br>Comprehension (to understand or know)<br>Consciousness (to be aware of, to be informed) | User value<br>Usefulness<br>Functionality |
| Interaction process | Efficiency | Control (to manipulate or be empowered) | Efficiency<br>Ease of learning<br>Ease of Use |
| Attitudes & Experiences | Satisfaction | - | Satisfaction<br>Affect/Likeability<br>Trust<br>Helpfulness<br>Awareness of PET related issues |

Table 3: Framework for the PET-USES questionnaire

Thus, by using the terminology of Hornbæk, one can for instance investigate the outcome of using a particular interface in terms of effectiveness of goal completion but also in terms of user value and what the user learns from the interaction.

This framework makes it easy to integrate the above-mentioned constructs in one model as well as adding further constructs if that should be deemed necessary. Practical considerations, such as time and effort to answer the questions, prevent the PET-USES to measure all of the above-mentioned categories in separate scales and thus several of the categories will have to be combined into more general domains.

# Chapter 3

# UI Representation of Privacy-enhancing Identity Management Concepts

This Chapter will give an overview of the developed privacy-enhancing IDM concepts as well as tests of different origin (usability, questionnaires, etc.) which were conducted during *PrimeLife*'s first project year.

## 3.1 Results of the Usability Laboratory Test

During the first *PrimeLife* project year, a formal laboratory usability test was conducted on the *PRIME* prototype (IPv3, Figure 3). In the following sections the results of this test, which was held according to the guidelines of usability evaluation [NM94] are presented.

The *PRIME* IPv3 was the final output of the *PRIME* project which was preceeding the *PrimeLife* project. Since *PrimeLife* was supposed to be adapting and basing on *PRIME* technology, it deemed important to test the existing technology in order to establish an overview from a usability perspective and to obtain valuable input for the first *PrimeLife* prototypes.

### 3.1.1 Introduction to the Usability Laboratory Test

This paragraph describes the results of the formal usability laboratory test of the *PRIME* prototype (IPv3) (Figure 3) which was held according to the guidelines of usability evaluation [NM94].

The goal of the task oriented usability tests (cf. [CKU08]) was to identify usability problems, problems with the information architecture and potentials for user interface and interaction improvement of the *PRIME* interface. The test was conducted with 10 participants at the facilities of CURE in Austria. The qualitative results obtained from

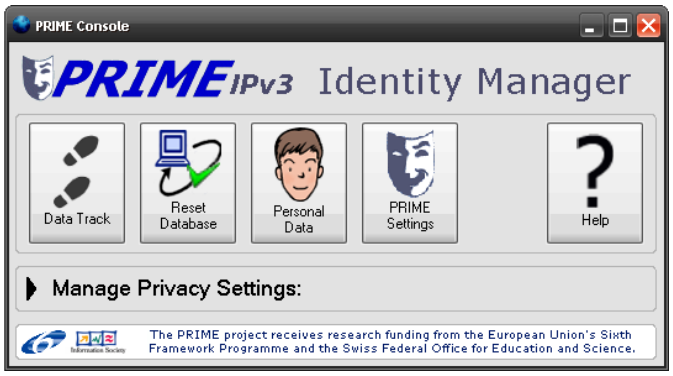



**Figure 3**: The *PRIME* IPv3 console as tested in the usability laboratory test.

the 10 participants allow to identify major problems and a tendency of issues. The main goal of this evaluation was the establishment of an overview of issues and problems.

The objectives of the test focused on the question if the proposed information architecture, interface design and interaction design meet the users' expectations and support their tasks. To cover these issues, test participants had to perform a set of 8 tasks. Variables such as the time to complete the task, occurring interaction problems and errors have been monitored. To measure test participants' subjective expectation and satisfaction, they had to answer a set of questions and fill in a questionnaire before and after the test. The results of the usability laboratory tests are the basis for recommendations of system improvements.

### 3.1.2 Problem Statement for the Usability Laboratory Test

The usability laboratory test has mainly addressed the following issues:

- Are users able to use the system intuitively?
- Do users feel safer using this system?
- Do users feel that the system is easy to learn and remember?
- Are users able to reach their goal using this system?
- Does the system support the user sufficiently?
- Can users gain a correct mental model of the system?
- Do users understand the functions of the system and are they perceived as useful?
- Does the system convey the importance of privacy?
- Is the wording clear to users?

The tests revealed problems related to the interaction with the *PRIME* interface and provide an extensive answer to these questions.

### 3.1.3 Executive Summary of the Usability Laboratory Test

The laboratory usability evaluation of the *PRIME* IPv3 revealed that the idea of self-monitored privacy protection and IDM is a function that is desired and highly appreciated. Furthermore also the possibility to track back personal data that has been disclosed in the past was a very valued feature of IPv3.

Although not all features were fully implemented, the usability tests have revealed some areas that are in need of improvement, such as the possibility to save settings in the login dialogue of the *PRIME* Playground, the search functionality of the data track, or the possibility to change settings of the *PRIME* console interface. A more detailed listing of the main issues discovered during the tests can be seen in Table 4.

| Issue | Explanation |
|---|---|
| Clarity, Transparency | - Hard to understand the deeper sense behind some functionalities<br>- Lack of descriptions and clear wording<br>- Unclear what application of the *PRIME* system should be used with what task<br>- *PRIME* console is easily confused with *PRIME* Playground |
| Efficiency, Wording in user's language, Feedback | - Too much information (especially in the login interface)<br>- Non-understandable information<br>- Overcrowded interfaces<br>- Non-understandable error messages<br>- Feedback is missing |
| Consistency | - Not all functions are fully implemented (e.g. data track)<br>- Missing sample-data for testing<br>- Inconsistent layout<br>- Inconsistent use of icons<br>- Inconsistent look and feel<br>- Appearance is not professional<br>- Inconsistent help-files (layout and content) |
| Flexibility, Efficiency, Memory load | - Use of different interaction paradigms (e.g. record slider)<br>- Non-intuitive interaction paradigms |
| Memory load | - Hidden menu-items and options (e.g. manage privacy settings) |
| Clearly marked exit | - No "close" buttons, many pop-ups (users ended up with 20 windows) |
| Trust | - Usability problems lead to a low level of trust in the interface |

Table 4: Main usability issues discovered through the laboratory usability tests of IPv3.

Especially the data track was widely appreciated as a great idea and the participants

were quite enthusiastic about its possibilities. Because of the simplicity and clarity of the displayed information, the record list was the preferred visualisation by most of the users.

As a result of the laboratory usability tests, a complete usability overhaul of the whole interface is recommended. This should not only boost usability but also enable users to build up trust. For the data track it is recommended to add search functionality and test with users again when the planned functionality is fully implemented.

Summarizing, more than half of the participants would feel safer using the *PRIME* interface and six test participants would use the interface in the future - given that the implementation would be completed and the interface would be made more self-explanatory and usable.

#### 3.1.3.1 PET-Uses

The PET-aspects scales used during the current investigation were: Data Management, PrivPrefs, Recipient, Action, and History which all were included to evaluate specific PET-related functionality of the software. The focus of the scales are:

- Data management: the extent the system makes it easier to store and organize personal information and credentials.
- PrivPrefs: the extent the system makes it easier to set general levels for data release and to what extent the user is informed of unwanted data dissemination.
- Recipient: the extent to which the system helps users evaluate the data recipients credibility and trustworthiness.
- Action: the extent to which the system clarifies when and what personal information is being released.
- History: the extent to which the system can show the user when what and to whom personal information has been released and what rights the user has in terms of access and control of this data.

General Usability is measured with the scales Ease of Learning, Ease of Use, and User Value as the possible response range is 1 to 7 it is noteworthy that the lowest scoring scale EaseOfUse got 4.3, exceeding the mid-point 3.5 with nearly one mark (see Figure 4). However, it is even more noteworthy that this scale received the lowest score of all scales in the PET-USES leaving quite some room for improvement in terms of usability. On a more positive note the scores on the EaseOfLearning scale indicate that the test participants think they grasp the concept of the software quite easily. Last but not least the test participants' response to User Value scale clearly shows that the software provides desirable functionality.

The focus of the PET-usability scales is both the functionality of the software i.e. does it do what it is supposed to do and to what extent the test participants gets a better understanding of privacy related issues. From this respect it is therefore interesting to see that the Action scale, which measures to what extent the system clarifies what personal information is being sent, scores high (see Figure 5). On the other hand, the Recipient

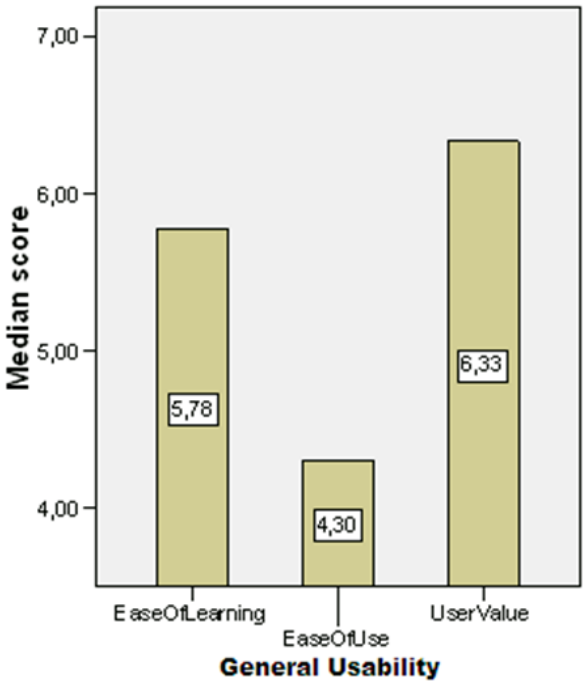



**Figure 4**: Median values of general usability scales (Ease of Learning, Ease of Use and User Value).

scale, measuring to the test participant understanding of the information recipient, score rather low, indicates that the recipient presentation and assurance evaluation needs to be reworked. Furthermore, the scale that scored the highest of all scales was History which measures the test participants' possibility to find out who received their data with the data track.

On a general level, an interesting point is the overall high scores, given despite the fact that test participants had great troubles completing the tasks due to, amongst other things, the lack of functionality in the prototype. Tentative explanations might be that test participants responded as they thought they would, had the console worked as they thought it should. Another possibility is that test participants are so happy with the value of the novel functionality (for instance with the data track), that they therefore responded favourably.

#### 3.1.3.2 Gaze Data

The hotspots in Figure 6 show seven test participants' gaze data during the *PRIME* Registration/SignUp task. The Xs indicate mouse clicks and the colour indicate the amount of gaze upon a given area with the highest amounts of gaze at the red areas.

In order to complete the task, test participants only needed information from the *PRIME* console. Given the large amount of gaze and click data outside the console,

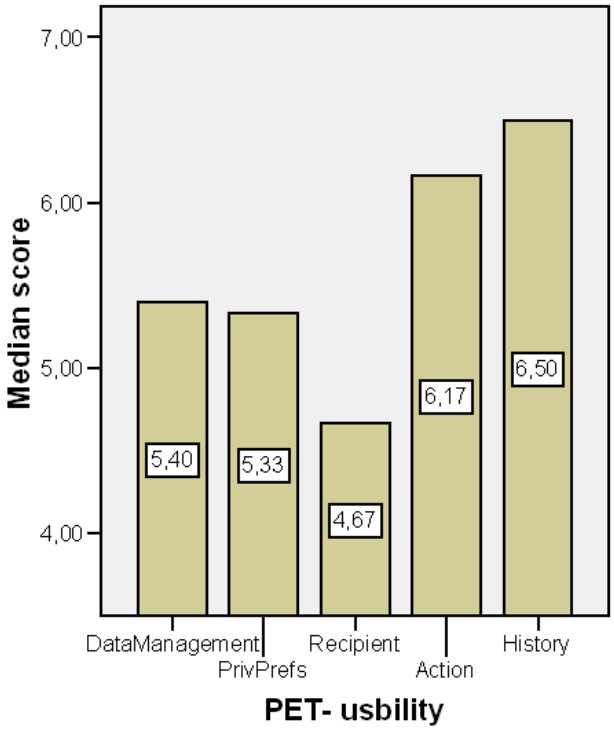



**Figure 5**: Median values of general usability scales (DataManagement, PrivPrefs, Recipient, Action and History).

this was apparently not clear to the test participants. Additionally, of the seven test participants included in this analysis, four finished the task by clicking the "Save Settings" button and one by clicking the "X" in the top right corner and three completed the task in the corrects way by clicking the "Next" button. Furthermore, the amount of clicking on the assurance evaluation error (circled green in Figure 6) shows that this is something that test participants want to fix but do not know how to accomplish. It is noteworthy that the system does not give test participants any other option than to mention and accept that eShopping failed on one of the criteria. Finally it is worth to point out that not many test participants have looked at the different tabs. This raises the question of how important the tabs and their information are. If the information should definitely be viewed by the user, another display approach should be chosen to emphasize this information.

Summarising, it can be stated that these behavioural patterns show that the interface is contra-intuitive, and that it is neither apparent to test participant what they should do to complete the task, nor where they can find the information they need to figure this out. The latter problem can partially be solved by using a "light box" i.e. greying out everything outside the console and thus making it clear that the console is the only source of information needed (Figure 7). The task completion issue shows that the interface is ambiguous and that the particular work flow needed has to be emphasised.

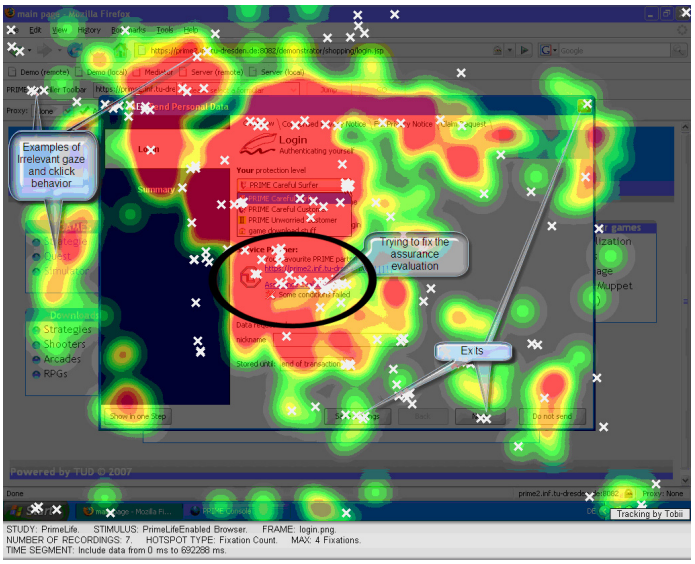



**Figure 6**: Hotspot of the *PRIME* Registration/SignUp task.

At a minimum the superfluous "Save Settings" button should be removed.

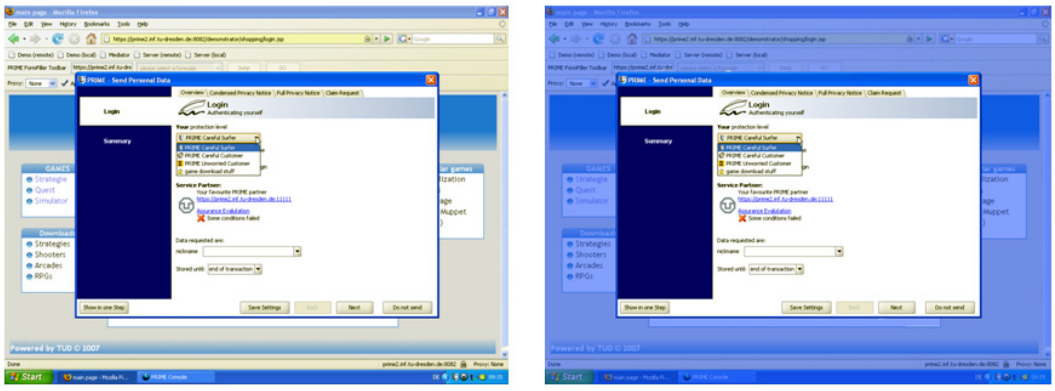


**Figure 7**: Example of how the *PRIME* Registration/SignUp console currently looks (left image) and how it would look with a light box (right image).

The hotspot in Figure 8 shows six test participants' gaze data during the Privacy Preferences task. In comparison with the previous hot-spot the most noteworthy aspect is the small amount of gaze and click-data outside the console. This shows that the test participants understand where they should be doing something to solve the task.

It is, however, not clear how this task should be completed. It took the participants an average of 3:10 minutes to find the "Manage Privacy Settings" button of which most time was spent clicking on the other buttons and exploring the following views looking for the Privacy Preferences (see Figure 9). Out of the six participants in this image,

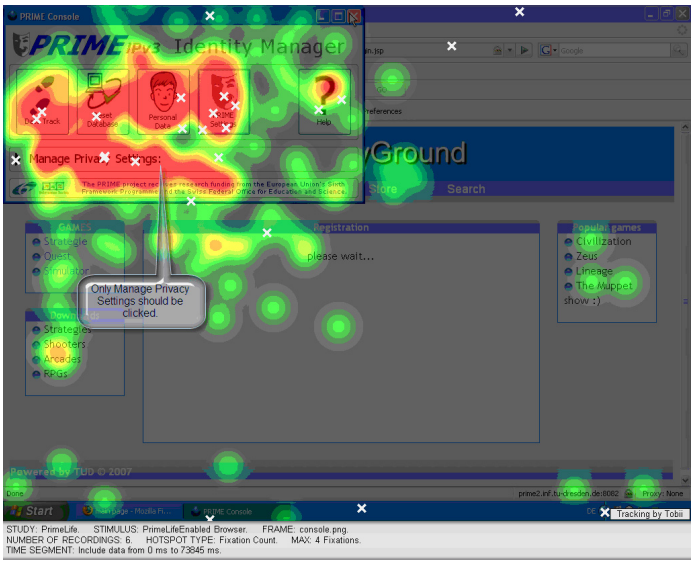



**Figure 8**: Hot-spot of the Privacy Preferences task.

five clicked the "*PRIME* Settings" button before the "Manage Privacy Settings" button, clearly indicating that this is a more intuitive action. This is most probably due to the fact that it was difficult to understand that the "Manage Privacy Settings" button was a button as it is an interactive element that occurs only once throughout the application.

This highlights a general problem of the application: there are too many different interactive patterns. Also, some of the different interactive patterns refer to nearly identical constructs, like the two different types of buttons on the Identity Manager console. Finally, some of the identical patterns do different things, such as the links on the "Send Personal Data" dialogue (Figure 10).

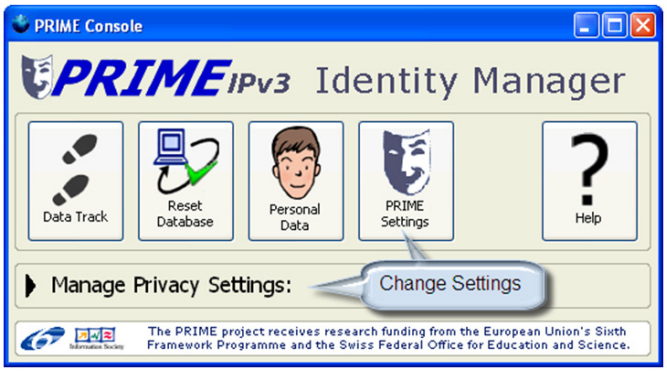



**Figure 9**: Instance of the Identity Manager and the different interactive patterns.

On the same note, in order to create a consistent test participant experience, all parts

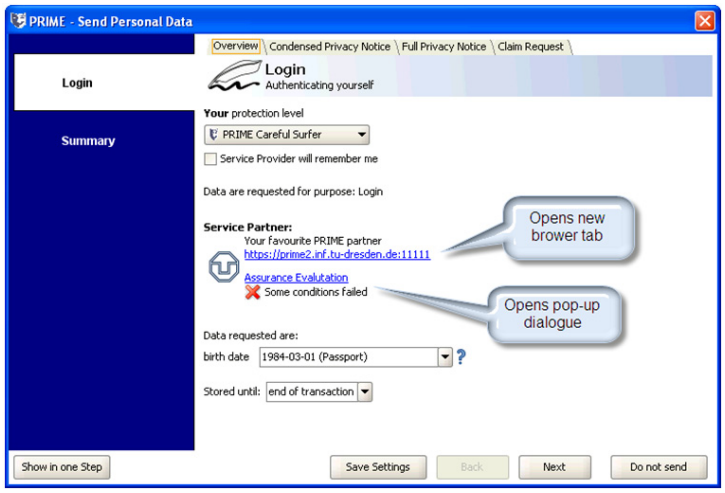



**Figure 10**: Instance of the Send Personal Data dialogue and the identical interactive patterns.

of an application should have the same look and feel. This is true, not only in terms of interactive elements and their functionality, but in all aspects of the application design.

### 3.1.4 Conclusions

The usability test has indicated some flaws as well as positive aspects of the *PrimeLife* interface. Although there are multiple usability issues the users' responses to the PETUSES clearly show that they appreciate the functionality and would like to use such an application during their everyday on-line activities. For example, the majority of users appreciated the possibility to be able to track data traces on the internet. The test participants remarked that there is a lack of trustworthy tools that help to monitor privacy protection and IDM.

Especially since some functionalities have not been entirely implemented, it was hard for the participants to understand a deeper sense behind some parts of the interface. Additionally the chosen wording and the interface itself were misguiding. Furthermore the users were overwhelmed by the amount of data presented to them in a rather unstructured way. Therefore they suggested to change the look of the interface in order to create a more consistent and better structured interface.

We strongly recommend a complete usability overhaul of the entire interface. In the course of this process basic interface design guidelines should be applied. These steps should not only boost usability but also enable users to build up trust (which can be measured using questionnaires and the PETUSES).

Concerning the icon with the footsteps, which was appreciated and told to be very clear and coherent, should be kept but adapted to a consistent icon-style. The basic idea of the data track should also be maintained, since the users especially liked the possibility to track their trace in the online world. Anyway we recommend adding search functionality and testing with users again when the planned functionality is fully

implemented.

Summarising, the test has shown that more than half of the participants would feel safer using the *PRIME* interface. Given that the implementation would be completed and the interface would be made more self-explanatory and usable, six test participants would use a future *PrimeLife* interface.

## 3.2 Mock-Ups of UI Representations

Since the beginning of the *PrimeLife* project, two different mock-up meetings were held. The first meeting was organised as part of the general meeting in Stockholm in June 2008. In this meeting different approaches for user interfaces were discussed with members of various Work Packages.

In order to agree on approaches for user interfaces in the various domains covered by the *PrimeLife* project (as discussed in the first mock-up meeting), an "extended" meeting with members of Activity 4 was held in Vienna in October 2008. The goal of this meeting was to discuss and present mock-ups for

- Credential selection (anonymous credentials)
- Send data dialogue
- Policy management (server- and user-side)
- Assurance evaluation/control
- Data track
- Legal aspects/requirements
- Scenarios

and to agree on further steps such as designs, mock-ups and testing. The following Sections provide an overview of current mock-ups, which have been discussed in the two meetings as described above.

### 3.2.1 Anonymous Credentials

A fundamental privacy design principle is data minimisation for transactions i.e. that the least possible amount of information is revealed between users and their communication partners (services sides or other users). This limits the communication partner's ability to profile users. This data minimisation principle can be derived from the EU Data Protection Directive 95/46/EC: The processing of personal data must be limited to data that are adequate, relevant and not excessive (Art.6 I (c)). Besides, data should not be kept in a personally identifiable form any longer than necessary (Art.6 I (e)).

Indeed, privacy of individuals is best protected if no personal data about them are collected or processed at all.

In *PrimeLife*, the use of anonymous credentials [CL01] helps to enforce data minimisation: If a user needs to provide some personal information e.g. for getting a service, the anonymous credential system can enforce that only the requested personal data are revealed. A credential is a set of attributes signed by the issuer of the credential and

bound to the credential owner. Traditional credentials (also called certificates) require that all attributes are disclosed together if the holder wants to prove certain properties. This makes different uses of the same credential linkable to each other. In contrast to traditional credentials, anonymous credentials make it possible for a user to prove only specific properties to a communication partner without revealing any extra information. For example, if a user has a governmentally issued anonymous passport credential with attributes such as his age and he wants to download a video which is only permitted for adults he can prove via some cryptographic zero-knowledge proofs with his credential just the fact that he is older than 18 without revealing his birth date or age or anything else. In addition, anonymous credentials have the property that multiple uses of the credential cannot be linked to each other. If, for instance, the user later wants to purchase another video which is only permitted for adults at the same video shop, he can use the same anonymous credential as proof that he is over 18 without that video shop being able to recognise that the two proofs are based on the same credential. This means that the two purchases cannot be linked to the same person.

A special challenge for HCI representations of anonymous credentials is therefore to illustrate the following two characteristics:

- Anonymous credentials allow proving only certain of its attributes or properties without revealing any other attributes stored in them. However, also information about the certifier is revealed (if the user uses for instance a governmentally issued credential, information about the government of the user (i.e. its nationality) is also revealed as meta-information)
- Multiple uses of the same anonymous credentials cannot be linked

These characteristics differ from the ones of real-world credentials, and therefore it is hard to derive good metaphors or UI illustrations that are well understood by the users. User tests conducted within *PRIME* based on earlier UI mock-ups for anonymous credentials showed that users often believe that a proof of "age $>$ 18" based on an anonymous credential reveals the full set of data contained in the source credential (and not only the fact that the holder is over 18).

#### 3.2.1.1 Credential Selection Paradigms

Service providers generally let the user choose between log-in using an existing identity or transmit a set of attributes for establishing the trust relationship (this statement is transmitted by a policy). We start with looking at the case where the user opts for transmitting a set of attributes.

The service provider asks for a set of attributes. The question now is how to let the user select the values for the required attributes. Usually also proof of the validity of the values has to be provided (which credential to reveal). There seem to be at least two different paradigms in selecting credentials, single attribute based and attribute group based. Both paradigms have in common that the user has a set of certified attribute-value pairs from different issuers (certified credentials).

In the **attribute based** approach, the user gets to select appropriate certifiers for each of the requested attributes. Selection of a specific certifier for one attribute may

lead to suggestions for certifiers for other attributes. These suggestions are based on the calculation of privacy issues (e.g. linkability, minimum number of certifiers, and minimum amount of collaterally revealed information (passport issuer as certifier reveals nationality)). This approach lets the user focus on attributes (and their proof).

In the **attribute group based** (plastic card based) approach, the system presents the user with a list of attributes that have to be provided (like above) and presents the user with a set of "cards" that contain the required attributes. What will be transmitted to the service provider is the set of attribute-value pairs and their certifier that meet the requirements. The user can select alternative sets of cards that meet the requirements. This approach requires the user to understand that not all data on each card is transmitted.

In both approaches the system will try to make sensible groupings of attributes (e.g. first name and last name always grouped) such that the user can easily select the appropriate certifier for the group in one step.

#### 3.2.1.2 Credential Selection

Based on the descriptions of credential selection paradigms and anonymous credentials there are a number of issues that need to be into taken account in order to construct an understandable UI-representation of credential selection. The process of credential selection can be divided into two separate parts, the selection of data to be sent and the summary representations of the selected data. During both parts, the level of anonymity must be transparent to the user so that he can make an informed choice of whether or not to send the requested data to the data-recipient. Irrespective of the level of anonymity, the UI-representations of credential selection is closely tied to the mental model of the credential selection paradigms. Thus, during the attribute based approach credential selection should be conveyed as a choice of specific attributes, whereas during the card based (attribute group) approach, credential selection should be based on a graphical representation of the card itself. The question of representation is also important during the summary of selected data as it is important that this UI conveys the principle of data-minimisation.

In sum then there are three main points that need to be taken into account in order to construct a comprehensible credential selection mechanism. The first pertains to users understanding of the concept of anonymous credentials and the two last to the mental model of credential selection and principal of data-minimisation

- Credential type: - Traditional (identity or attribute certificate) vs. Anonymous
- Selection mechanism: - Cards vs. Attributes
- Summary representation style: - Icons vs. Text

#### 3.2.1.3 Mock-Up Proposals

As described in Section 3.2, in our ongoing work to investigate the effects of possible UI variations for credential selection and user comprehension of Anonymous Credentials and data minimisation a number of mock-ups have been developed and are currently under implementation. These will be tested during the spring of 2009 at KAU and CURE.

The issue of the level of anonymity and data minimisation is in many ways the most central but also the most difficult to convey to the user. This is mainly because the concept of anonymous credentials differs so much from the users' current understanding of the credential concept. Thus, the level of anonymity (e.g. date of birth or age $> 18$) must be transparent in the description of the requested data both during the selection and summary of credential selection (see Figure 11 for examples of data request during the credential selection). During the user trials, groups of users will be given different scenarios which include the use of various levels of desired anonymity

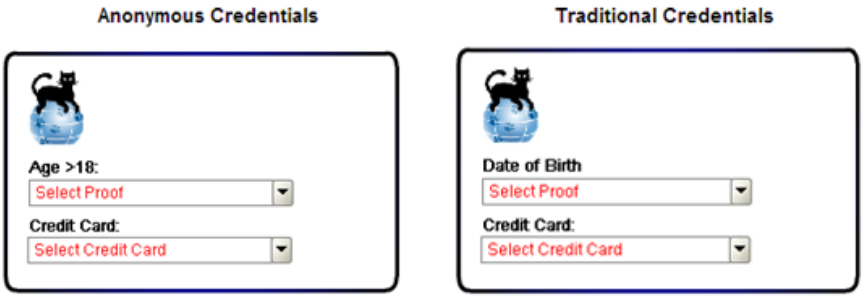



**Figure 11**: Examples of data requests during the selection of Anonymous Credentials (Age $> 18$) and Traditional Credentials (Date of Birth).

The issues of credential selection paradigms and mental models is also tightly knit to the users' current understanding of non-electronic credentials. On good grounds, proponents of the plastic card paradigm argue that this is easily understood by users as this mimics what they already know and use most every day. And thus, explaining the basic idea of digital credentials is easily done by comparing them to their plastic predecessors. However, in contrast to the objective of data-minimisation, showing a plastic card always results in the revelation of all information on the card and thus the ease of explanation might be a pyrrhic victory. In order to investigate which of the two paradigm makes it easier for users to understand the principle of data-minimisation two UIs are proposed where selection is either done by clicking on a representation of the full card containing the desired attribute or by choosing the attribute from a drop-down list containing the possible sources of the attribute (see Figure 12 for examples).

Lastly, there is the issue of how to represent the summary of selected credentials. This presentation should follow the same pattern as described before, i.e. the actual data request and response in order to achieve transparency of level of anonymity. The question here is rather how to represent the source of the credential and still convey the minimal data release. The central issue is if users will be biased by their offline use of plastic cards so that they will interpret an icon of a plastic card (as used in the left card of Figure 13) as the release of all attributes associated with this card. This will be tested by contrasting a summary presentation containing an icon of the source credential with a presentation where the source credentials are instead referred to by text only (see Figure 13 for examples).

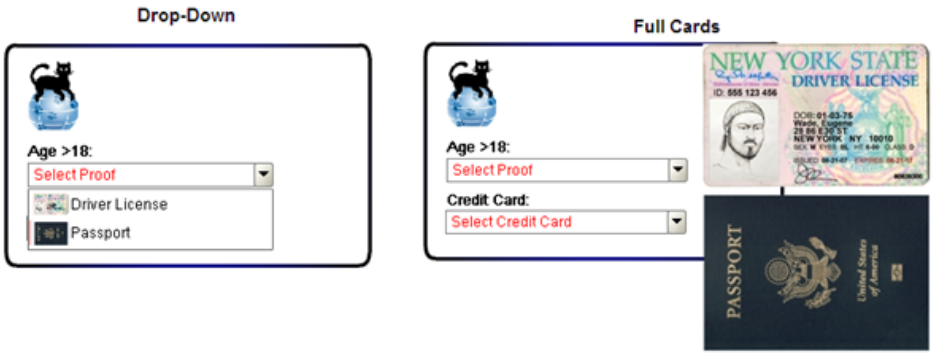



**Figure 12**: The selection mechanism of the attribute based (Drop-Down) and the group-based (Full Cards) paradigms during the use of an Anonymous Credential.

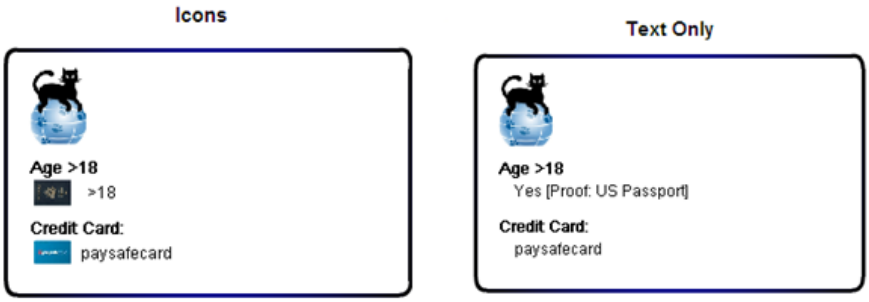



**Figure 13**: The selected credential summary representations either referring to the source credential by the use of an icon or by text only.

#### 3.2.1.4 Concluding Remarks on the Evaluation of Credential Selection Mechanisms

A central problem of introducing UIs of selection mechanisms of anonymous credentials lies in the leap of thought required of users in order to grasp the novel functionality of the anonymous credentials themselves. Therefore it is important to differentiate between the understandings that it is possible to prove only a specific attribute such as date of birth and the possibility to prove a generalised attribute such as older then 18. By including test scenarios where traditional and anonymous credentials are contrasted it is possible to distinguish between errors based on a misconception of the concepts of anonymous credentials and data-minimisation. Also, by including the group based and attribute group based credential selection paradigms in the same test it is possible to draw conclusions on which mental model makes it more easy to understand the introduced concepts and principles.

### 3.2.2 Privacy Preferences Presentation

One of the biggest issues of the *PrimeLife* project is to develop an efficient way on how to display information in a usable way that matches the high security criteria. More detailed information on privacy preferences (short: PrivPref) and their use within *PrimeLife* can be found in Section 5.

Using the PrivPref-approach (as described in Section 5), Mike Bergman (TUD) developed two different prototypes - a dynamic and a static interface - that were modified together with CURE to be tested in the virtual usability laboratory.

The virtual usability laboratory is an online testing framework, which was developed by CURE for the *PrimeLife* project[1] (see Figure 14). It is secured with a user name and a password, which allows to restrict the access to selected test subjects only. On this platform different small studies and surveys can be offered to the users.


**Figure 14**: The virtual usability laboratory developed by CURE.

In order to evaluate the platform itself (proof of concept of its functionality) and to test the initial mock-ups as discussed above, both prototypes were integrated into the Google Mail login-interface (Figure 15 and 16). The entire test setup was designed in German, since the target audience of CURE's test user database was Austrian. In both interfaces, the users were asked to log into the Google Mail interface with a given user name and a given password. On the screen following the login interface, the users were asked questions about the interface just experienced. A link to each prototype was sent to 25 randomly selected internet literate users from CURE's test user database.

#### 3.2.2.1 Results from the Evaluation

For both mock-ups we could accomplish a response rate of 28 % (7 users each). The results indicate that the dynamic box is easier recognizable than the rather static yellow bar, which was only recognized by 43 % of respondents.

Concerning the security of the information disclosed using the Google Mail interface, the users indicated that both interfaces do not appear to be very trustworthy, with the yellow bar interface inspiring slightly more confidence than the dynamic box. The

[1] `http://primelife.cure.at/`


**Figure 15**: The Google Mail login-interface with the yellow bar mock-up.


**Figure 16**: The Google Mail login-interface with the dynamic box mock-up.

interface appeared to be quite consistent for both prototypes, nevertheless the questions concerning the safety of the information disclosed and the trustworthiness of the interface, the ratings were quite high (indicating low trust and security). The impression the two interfaces made on the participants can be seen in the diagrams in Figure 17.

When asked about the level of information obtained from the interface, all users who tested the yellow bar interface indicated that they did not feel well informed about the interface and in case of the dynamic box, only 29 % of the users meant to be well informed. In case of the dynamic box interface, the users indicated that they expect their data to be handled rather irresponsibly, with an average rating of 4.43 (1 = responsible, 7 = irresponsible). Also in case of the yellow bar, 3 users were convinced that their data would be handed over to third parties.

A possible bias towards Google and their interface cannot be denied and further studies are to be conducted in order to investigate influential factors on trust in data requiring interfaces. Nevertheless it appears to be important that the privacy functionality

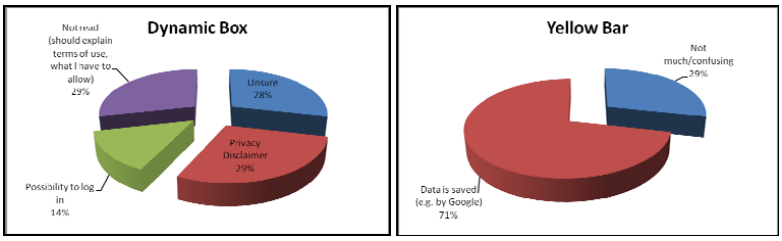



**Figure 17**: The user's impression of the context of the different interfaces.

is appropriate to the context it is used in. Concerning the clarity of the terms employed in the interface, the participants indicated that especially "careful surfer", "save" and "please do not save" are understandable.

#### 3.2.2.2 Conclusion and Next Steps

The trial evaluation of the virtual usability laboratory has proven to be an efficient way to test small prototypes with a rather larger audience in a very short period of time. With a response-rate of 28 % and an average response time of about 3 days, our hypothesis that the virtual testing shortens the evaluation process for certain prototypes, is met. Especially since we are not testing exhaustive prototypes the time a user needs to complete the study is minimized (e.g. 15 minutes). Therefore we are able to test even small prototypes and not functioning mock-ups with a considerable number of users, which allows us to collect even more user feedback throughout the development process.

Currently only few scientific works are available on certain parts of secure interfaces. We therefore want to advance current research in this area. The findings of the online study reveal that users rather react to dynamic content (dynamic box) that is visible when needed than to static content that is "always there". This might be caused by the user's tendency to focus on the task itself without regarding additional information such as long privacy policies. The dynamic box prototype was developed according to HCI guidelines, since the feedback is only provided when entering the login-dialogue (i.e. when needed).

Both interfaces tested appeared to be consistent, nevertheless the users have expressed concerns about the safety of the disclosed data. It appears to be important that the privacy functionality is appropriate to the context it is used in.

Summarising it can be stated that asynchronous usability testing is a valuable design tool for HCI security (especially since there is not much existing knowledge available). Furthermore the evaluation has revealed the need for further research on the issue of secure and usable interfaces. The results of the study will inform the creation of *PrimeLife*'s HCI security pattern collection.

# Chapter 4

# HCI for Trust and Assurance Evaluation

## 4.1 Introduction

"Trust is important because if a person is to use a system to its full potential, be it an e-commerce site or a computer program, it is essential for him/her to trust the system" Johnston et al. assert [JEL03]. One objective of the *PrimeLife* user interfaces addressed by *PrimeLife* Task 4.2.1 is to mediate trust information, which allows users to establish reliable trust in communication partners (services sides or other users) and which effectively alarms them about non-trustworthy contacts.

Usability tests of *PRIME* prototypes as well as research results of others have shown that there are problems to make people trust the claims about the privacy-enhancing features of the systems (see [PFHND+05],[GS05]). The HCI research in *PrimeLife* approaches this problem in order to enhance the users' trust in *PrimeLife* and its back-end systems, by investigating the challenges to communicate reliable information about trustworthiness and assurance (of providing the stated functionality) of communication partners. For this, an interdisciplinary approach has to be taken to investigate not only the technical options but also the social factors and HCI aspects for influencing trust (see [ACC+05]).

During the process of trust negotiation, the user can request to obtain information about the trustworthiness of his communication partner. Trust negotiation involves the user releasing data (e.g., proving that he is over 18 with a credential) in order to get access to a resource or service after the communication partner has provided evidence that he is sufficiently "trustworthy" as required by the user's preferences, e.g., by providing privacy seals, or evidence regarding his reputation. These evidences or so-called claims provided by a communication partner (usually positive trust claims) can be complemented by further trust information (in particular evidences of non-trustworthiness) that could be requested by the user from other third trustworthy monitoring parties, such as data protection commissioners or consumer organisations. For allowing the user to do well-informed decisions, this trust and assurance information provided by the communication

partner or other third parties needs to be evaluated and presented to the user in an appropriate and user-friendly manner at the moment when he is requested to release personal data to the communication partner.

Within its first project year, Task 4.2.1 has as mentioned already mainly done research on meditating trust and assurance information of services sides in the so-called "Trust Evaluation Function", which could, e.g., be used by users to evaluate the trustworthiness and assurance of e-commerce sides, e-government sides or sides of social community providers (such as Facebook or MySpace). Hence, our first research results presented in this Section also focus on trust and assurance HCI for client-server constellations. In Section 4.6, we will however also discuss the HCI challenges for representing metrics as trust information on peer-to-peer communication partners, such as social network users.

## 4.2 Challenges

Designing the UI for a Trust Evaluation Function poses several challenges that need to be addressed. In particular, we have to find appropriate trust metrics that need to be evaluated, aggregated and presented in a manner that is helpful, appreciated and well understood, i.e. not misinterpreted by the end user. For this, the following issues need to be addressed:

### 4.2.1 Find suitable trust and assurance parameters and meaningful metrics

An important question to begin with is: What are suitable parameters for measuring the trustworthiness of communication partners and for establishing reliable trust? For this we have to take social factors influencing trust and available trust measures into account.

The model of social trust factors which was developed by social science researchers in *PRIME* and presented in [ACC+05] states that trust in a service provider can be established by monitoring and enforcing institutions, such as data protection commissioners, consumer organisations and certification bodies. Hence, the following parameters can be suitable for establishing reliable trust:

- **Privacy seals** certified by data protection commissioners or independent certifiers, such as the EuroPrise seal, the TRUSTe seal or the ULD Gütesiegel, provide especially suitable information for establishing (and therefore positively influencing) user trust. Such privacy seals certify the privacy compliance of the service provider's IT system with data protection regulations or privacy principles issued after a successful audit. Seals digitally signed by its certifier can be either provided by the service provider during the process of trust negotiation or requested/downloaded by the user's PrimeLife system from the certifier's side.

- Static seals such as privacy seals can be complemented by **dynamic seals conveying assurance information about the current security state** of the system and its implemented privacy and security functions. These are generated in real-time possibly by tamper-resistant hardware chips of the service provider's system

and can be provided during the trust negotiation process. Dynamic seals that are generated by tamper-resistant hardware can be regarded as third-party endorsed assurances, as the tamper-resistant hardware device can be modelled as a third party that is not under full control of the communication partner.

Further information sources by independent trustworthy monitoring organisations that can measure (and negatively influence) the trustworthiness of services sides can be the following parameters:

- **Blacklists**, i.e. lists of companies that are "blacklisted" provided by some consumer organisations, such as Konsumentverket in Sweden. (Note however that whereas consumer organisations is some European countries, such as Denmark or Sweden, publish such blacklists, consumer organisations of other countries (e.g., France) are not able to publish such blacklists due to legal restrictions).

- **Privacy alerts** about organisations that are violating privacy, which are for instance provided by data protection commissioners in some countries. Also self-reports, which organisations that conducted privacy violations or had security incidents need to be provided in some countries, could be referenced to in privacy alert lists. In order to avoid confusing users with extensive warnings (see also 4.2.4 for more on the problem of misleading warnings), privacy alerts used for trust evaluations should warn only about serious privacy breaches and issues that have not been addressed and solved yet by the responsible party.

Further trust measures that can either positively or´negatively influence trust can be **reputation metrics** that are based on the user's ratings of a communication partner's privacy and business practices as experienced by the rating users. Reputation systems, such for instance the one in eBay [1], can however often be manipulated by reputation forging or poisoning. Besides, the calculated reputation values are often based on subjective ratings by non-experts, for who it might for instance be difficult to judge the privacy-friendliness of communication partners. Nevertheless, for peer-to-peer applications such as in virtual communities, reputation metrics might be the most suitable means for measuring trust, as the other trust parameters presented above can usually only be used to evaluate the trustworthiness of organisations (service providers) and not the one of private persons. These problems are also at least partly addressed by a multilaterally secure reputation system [Ste08] as it will be developed within PrimeLife.

### 4.2.2 Illustrate parameters with different semantics and scopes

Trust and Assurance parameters can have different scopes. Besides, the fact that information about parameters is available or not, or that criteria are fulfilled or not, can have different semantics.

The user's trust in a services side will depend both on the side's privacy and business practices – i.e. different aspects have to be measured. Parameters "Privacy seals", "Supports *PrimeLife* functions", "Mentioned in privacy alert lists" that we have chosen for our mock-ups (see below) measure the trust that users can put into that their data

[1] `http://www.ebay.com/`

are processed in a privacy-friendly and lawful manner. The parameter "Blacklisted" in turn measures the trustworthiness of a services side as a business partner. Users need to understand that privacy and business reliability are different trust categories (e.g., an eShop that is a reliable business partner could still misuse its customers' personal data or vice versa).

Moreover, the evaluation results that a side is not listed on blacklists or on privacy alert list are at least positive indications for the trustworthiness of a side, whereas the result that a side has no privacy seals, or that the privacy seals have expired, and information that *PrimeLife* functions are not supported is not anything positive. However, the absence of seals and support of *PrimeLife* functions cannot be interpreted as a negative ("bad") trust evaluation result either, as privacy seal evaluations and systems with implemented *PrimeLife* functions are very rare nowadays. Even privacy-friendly organizations today usually have no systems supporting *PrimeLife* functions or systems that have gone through a privacy seal certification, and thus would fail those criteria. This situation could however change in future.

A challenge for the user interface is to illustrate these different parameters and their different scopes and semantics in an understandable manner.

### 4.2.3 Find intuitive icons

Trust measures should also be illustrated by good policy icons, which can increase the learnability and may allow users to faster recognise the evaluation results. As already mentioned in the *PRIME* HCI Guidance deliverable D6.1.f, icons have to be carefully chosen and tested, so that they are intuitively understood by the users. That this may be a challenge is illustrated by the following example: For our mock-ups, we had initially illustrated the fact that a side has not a specific privacy seals by a crossed-out seal logo. Early expert evaluations of our mock-ups showed however that this could be misunderstood as an indication that the side has been certified for that seal and failed the certification. Hence, a seal with an overlaid question mark might be more appropriate. However, our usability tests showed that such an icon was not understood by many test users (see below).

### 4.2.4 Address usability problems discovered in previous tests

Furthermore, our trust evaluation function needs to address the following problems observed from usability tests of *PRIME* prototypes, which might even lead to reduced trust in a system if they are not properly treated:

- **Users have difficulties to differentiate between user and services sides**

  This problem was already detected in the usability tests of early *PRIME* prototypes (*PRIME* deliverable D6.1.b). The usability tests of the *PRIME* integrated prototype IPV3x also revealed that the user interfaces of the *PRIME* assurance evaluation function did for many test users not make clear enough that the services side and not the user side was evaluated. The consequence was that although the assurance evaluation function had the objective to enhance trust in *PRIME*, test scenarios with negative assurance evaluation results led to a reduced trust of test users in the *PRIME* system.

- **Extensive warnings can be misleading**

  The assurance evaluation function in *PRIME* displayed warnings also in cases that services sides had no privacy seals or were not implementing *PRIME* functionality. These warnings confused many users who were unsure how to react on them. The fact that a side has no seal and is not running *PrimeLife* is usually nothing a user needs to be concerned about – this is the case for the majority of services sides today. As discussed above, having a seal and implementing *PrimeLife* functions is definitively a positive trust indication, whereas the absence of seals and *PrimeLife* functionality support cannot be interpreted as a negative trust evaluation result.

## 4.3 Design Principles for our mock-ups

For the design of our trust evaluation mock-ups that were produced for our first iteration of usability tests, we followed the following design principles comprising general HCI principles as well as design principles, which should in particular address the challenges and problems discussed in the previous Section.

### 4.3.1 Use a multilayered structure for displaying evaluation results

In our mock-ups, the trust evaluation results are displayed in increasing details on multiple layers, in order to prevent an information overload for users not interested in the details of the evaluation (see Figure 18).

On the top layer, only the overall evaluation result is presented to the user in situations when he is requested to release personal data to a communication partner (i.e., in the "Send Personal Data?" window). The overall result is shown in form of a coloured emoticon accompanied by a short textual description (see below and Figure 18). Users that are interested in more details and the reasons for the overall results can click on "Trust evaluation result" to get to the second layer displaying the individual evaluation results of the four evaluation parameters that are referring to privacy alert lists, blacklisting, awarded privacy seals, support of *PrimeLife* functions. The third layer with the details of the individual evaluation results can then be reached from the second layer by clicking the "Expand" button, or by expanding the view on results for certain parameters only.

### 4.3.2 Use a selection of meaningful overall evaluation results

For simplification, the evaluation results are summarised into three possible overall results: "good", "not bad", and "poor". These results that already provide a semantic by their naming should be more meaningful than for instance percentages as used by reputation metrics such as in eBay or WOT[2] – Web of Trust (How should, for instance, a reputation rating of 92% be interpreted by a user?). These names were chosen for alarming the users only in cases that something negative can be reported and for also informing them about positive trust indicators.

[2] `http://www.mywot.com/`

The following algorithm is used for calculating the overall results that are displayed on the top layer:

- A side is rated as "poor" (illustrated by the icon Poor ☹) if it is either blacklisted or mentioned in privacy alert lists;
- A side is rated as "good" (illustrated by the icon Good ☺), if nothing bad can be reported (i.e., the side is neither blacklisted nor appearing on privacy alert lists) and something positive can be reported (meaning that the side has been awarded a privacy seal or supports *PrimeLife* functions);
- A side is rated as "not bad" (illustrated by the icon Not bad 😐), if no positive (the side has no privacy seals, no support of *PrimeLife* functions) and no negative (the side does not appearing on privacy alert lists or blacklists) evaluation results are reported.

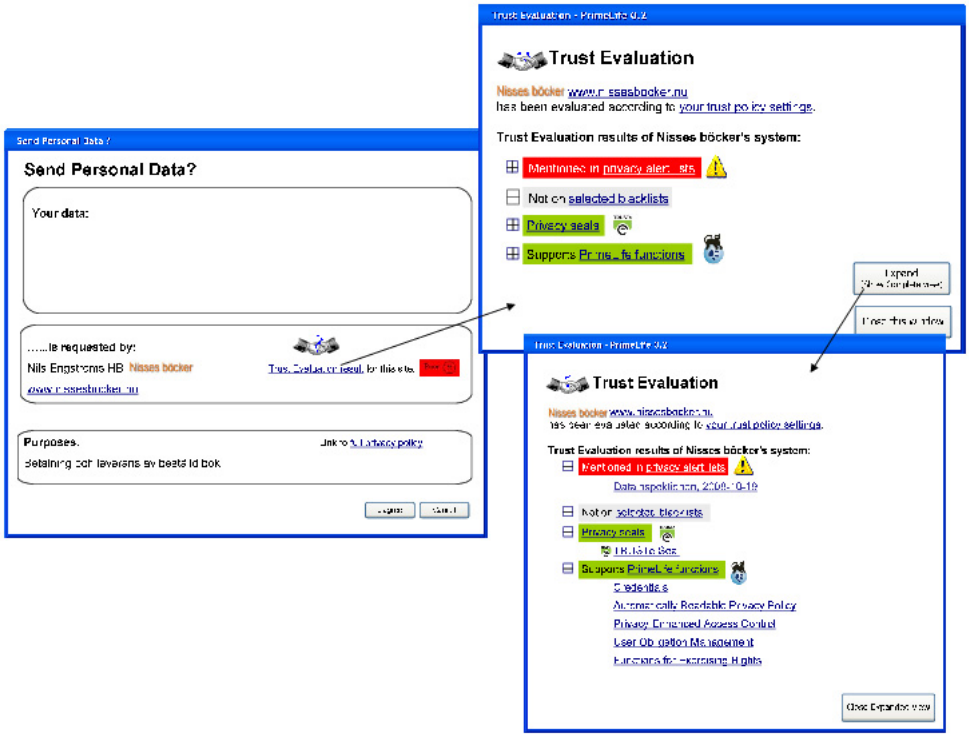



**Figure 18**: Mock-ups providing Multi-layered Trust Evaluation Presentation

### 4.3.3 Make clear who is evaluated

The user interface should make very clear that the services side and not the client side is evaluated. For showing this, our mock-ups are clearly speaking about the trust evaluation results "for this side" on the top level after naming this side. The fact that the trust evaluation results refer to the services side is also made clear by putting it into the box of the "Send Personal Data?" window displaying information about the data requester, i.e. the services side.

As illustrated in Figure 1(left side), the "Send Personal Data?" window is also structured in three areas referring to the data requested, the services side who is requesting the data, and the purposes. The trust evaluation result is placed in the area for the data requestor to make the relation even more clear.

On the second and third presentation layers, the evaluation subject is also clearly stated by the wording "[Company] has been evaluated..." used in the UI.

### 4.3.4 Use several UI concepts for informing users

In our mock-ups, we use the different UI concepts text, colouring and icons in combination, for informing the user about the evaluation results in an easily and intuitively understandable way. The text states the evaluation results unambiguously, while the colours "red", "green" and "grey" in addition mark "poor", "good" and "not bad" overall and individual evaluation results. The additional icons should enable users to quickly grasp these evaluation results.

The following icons were chosen:

#### 4.3.4.1 On top layer:

- For the trust evaluation function:

- For the overall evaluation results: (see above):


#### 4.3.4.2 On second and third layer:

- For alarming the user:

- For the evaluation result that a side has a privacy seal (TRUSTe seal, ULD Gütesiegel, EuroPrise seal):

- For the evaluation result that a side has not a specific seal or that there is at least no information about awarded seals (grey seals with a question mark):

- For the evaluation result that a seal once awarded for a side has expired (grey seals with an hour glass where the sand has already been running through):

- For the evaluation result that the services side supports *PrimeLife* functions (illustrated by the *PrimeLife* logo):

- For the evaluation result that the services side system does not support *PrimeLife* functions (crossed-out *PrimeLife* logo):

### 4.3.5 Inform the user without unnecessary warnings

As described above, users should only be alarmed about negative overall and individual evaluation results that they should worry about, i.e. in the cases where sides are blacklisted or appeared on privacy alert lists. In these cases, the overall evaluation result "poor" with a sad-looking emoticon and a red background colour is used. Also on the second layer, the individual evaluation results "Mentioned in privacy alert lists" and "Blacklisted" have an alarming red background colour and an alarm icon is displayed next to the text.

"Good" evaluation results are coloured "green" and if nothing good or bad is reported, "grey is used to symbolise that no positive and no negative evaluation results are reported.

For previous *PRIME* mock-ups of an assurance evaluation function, we used the traffic light metaphor with a yellow background colour if criteria were only partially fulfilled or if information about them was missing. The colour yellow is however symbolising a

state right previous to an alarm, which is thus not an appropriate analogy, as in those of partially fulfilled criteria or missing information nothing bad can be reported. The yellow colour might therefore unnecessarily warn or even confuse the users. Hence, instead of a yellow we have chosen a more neutral grey for those cases.

## 4.4 First usability tests and results

First usability tests of our mock-ups were performed in January 2009 in the Ozlab testing environment of Karlstad University with ten test persons. These tests took place in Mini-Ozlab instead of using the traditional Ozlab setup with a one-way mirror, which made it possible for the testleader to make notes about the test persons' reactions. Screen actions were also recorded and later analysed. Besides, post test interviews were performed.

The results of our first tests can be summarised as follows [Lin09]:

- Most participants seemed to understand the "Send Personal Data?" user interfaces and presented top-level trust evaluation results quiet easily. They thought that the UI was explicit and clear, with no distracting objects. The participants liked that the requested data were presented to them explicitly in "Send Personal Data?" before they decided to send their data or not.
- The "Good" and "Poor" emoticons on top level were also clearly understood by all users. Only the "Not bad"-emoticon was by some test participants interpreted as confusing (more reflection on this below).
- The colours red and green in the prototype (both on icons and over text) were all understood correctly by the participants.
- The icon for alarming the users was also correctly understood.
- As many as 6 out of 10 participants like the function they tested to be called "Trust Evaluation".
- All participants said in the interviews that they would like to use a *PrimeLife* prototype including a Trust Evaluation function that is similar to the one that was tested.
- All participants also clearly understood that the services side and not the user side was evaluated

However, the tests also revealed a couple of usability issues that need to be addressed by our next iteration of mock-ups:

- The more detailed trust evaluation results on the second layer were harder to understand for most test persons. Some thought that an overall "Poor" result with both red and green colours on the second layer (e.g. for one test scenario, where a side that supports *PrimeLife* functions was "blacklisted" or for the scenario illustrated in by the mock-ups in18) was confusing and was seen as a contradiction.
- The seal icons with question marks were hard to understand for most participants. All test participants misunderstood the seal icon with an hour glass.

- Some participants took a bad trust evaluation result on the parameter "Blacklisting" more serious than on "Privacy alerts". One comment from an interview with a test person was: *"Alerts are warnings, but when you are blacklisted then it is really serious - this makes you think twice before sending my data".*
- The "Not bad" evaluation result was hard to understand for some participants. For instance, one test person stated: *"According to the detailed result there is not result at all. Thus "Not bad" can mean "not evaluated".*
- The crossed-out *PrimeLife* icon was confusing for some participants and made them suspicious. *"[... ] Especially the cat icon reinforce my insecurity"* stated for example one participant.
- The grey colour (both on icons and text fields) was confusing for several participants. The participants gave different explanations of how they understood it, which included (note that nevertheless the first three answers listed below were at least partially correct):
  - *"The first row means that this control is not evaluated, or that the website has done nothing wrong. I can't say which answer is correct according to how the result is presented to me".*
  - *"This means that the website is not evaluated properly[...]"*
  - *"The details show that there is no information at all, thus you don't know if you can trust the website or not".*
  - *"Grey means either that I have not made any settings about this, or that PrimeLife thinks that this website is trusted (after controlling it). I am not sure which answer is the correct".*

## 4.5 Related UI approaches

Examples for related trust evaluation functions, which both measure reputation based on user ratings, are for example WOT and TrustPlus[3].

WOT is a browser plugin used for rating and evaluating other web sites by the categories "Trustworthiness", "Vendor Reliability", "Privacy" and "Child Safety". A "poor" or "very poor" rating in any area will trigger a warning by default. However, users can also customize their level of protection and can for instance also be warned if no ratings are available at all. WOT displays ratings for the four categories and an overall rating by coloured circles. Also the interface for soliciting user ratings uses the colour metaphors dark green (best rating), light green, yellow, light red, dark red (lowest rating) (see Figure 19). Relying only on colours as a UI technique for informing users has however the drawback that it is not usable for users with a colour-blindness handicap. Besides, the semantics of the colours, and particularly the yellow colour, might be interpreted differently by different users.

TrustPlus is a system for rating the other users based on previous transactions (i.e. in their roles as sellers, buyers), interactions (e.g., chatting, dating or relationships

[3] `http://www.trustplus.com/`

(e.g. friends, family member). It uses more advanced scheme of six different trust symbol icons that do not only differ by colour by also by their form (see Figure 20) to symbolise trust ratings on a hierarchical scale from “do not trust” to “most trustworthy”. For our purposes, however, we think that the less fine-grained scale with only three values that we are proposing will be expressive enough and easier to grasp by the users.

Both WOT and TrustPlus have the drawbacks of typical reputation systems as discussed above, i.e. they can be manipulated by reputation forging or poisoning, and often provide results of a limited reliability as the calculated reputation values are based on subjective ratings by usually non-experts.

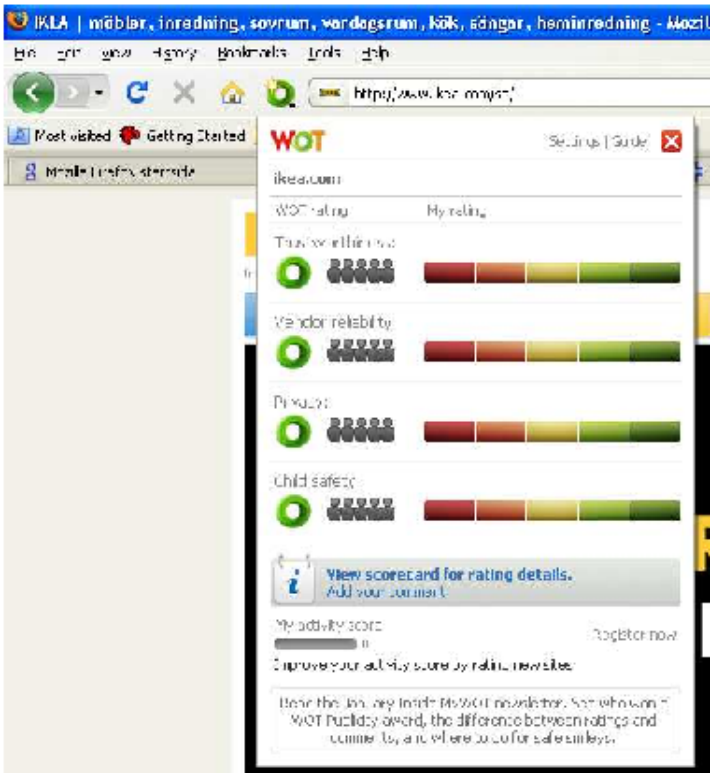



**Figure 19**: WOT User Interface for evaluating a side trhough user ratings

## 4.6 Outlook

### 4.6.1 Next iterations of mock-ups and tests

We are currently elaborating the next iteration of trust evaluation mock-ups, which should address the usability problems that were observed in our usability tests. For this, we are currently re-investing our icons and the presentation of evaluation results that are now coloured “grey”. Besides, we structure the trust parameters visible on the second and third layers into the categories “Business reliability” (comprising the parameter “blacklisted”) and “privacy (comprising the parameters of security&privacy

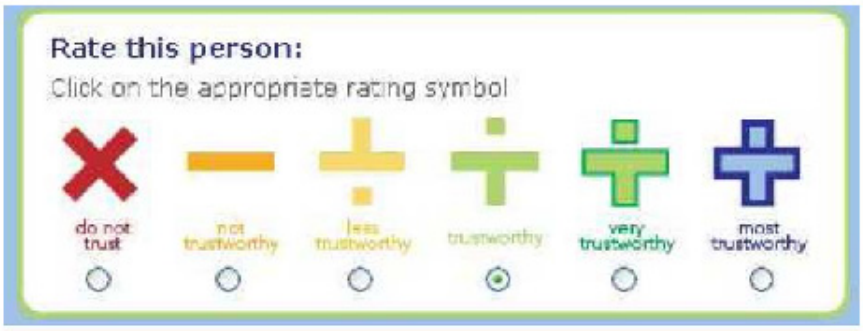



**Figure 20**: TrustPlus Inc. rating symbols

alert lists, privacy seals and *PrimeLife* function support)(see Figure 21). This structure should explain better the different semantics of our parameters and that scenarios with companies that are "blacklisted" for bad business practices, even though they have a privacy seal and/or support *PrimeLife* functions do not have to be contradictory, as they refer to different aspects of trustworthiness. These next iteration of mock-ups are soon tested at Karlstad University's Ozlab. All tests will also be repeated at CURE's usability lab, which will allow to compare tests results from a cultural perspective.

### 4.6.2 Mediating reputation metrics for social community users

Within the next reporting period, we plan to develop and test also UI proposals for presenting reputation metrics for social community users. For this, we have started to discuss HCI challenges and elicit requirements in cooperation with *PrimeLife* Work Package 2.2.

In particular, we need to further investigate the following aspects:

- How should ratings and the absence of ratings be interpreted, accumulated and presented in a meaningful way? As discussed above, reputation systems as used in eBay or WOT often accumulate all ratings in form of percentages, which are often not very meaningful for end users. For reputation systems where users have to be afraid of bad "revenge" ratings of their business partners, the fact that a business transaction was not rated at all could be an indication for a negative business experience. More indicative reputation metrics should for instance at least also include information about how many ratings were given for how many business transactions, and thus how many ratings are missing.

- Will pseudonymity of persons being rated influence their trustworthiness as perceived by others? An interesting research question is whether users that act under their real identity or always use the same pseudonym are more trusted by others than users that switch pseudonyms (i.e. that behave more privacy-friendly). For enhancing trust in pseudonymous users, the fact that the identity provider of an anonymous credential can trace back a misbehaving pseudonymous user should be illustrated to the other users.


**Figure 21**: New iteration of Trust evaluation mock-ups (2nd layer) to be tested next.

- When and where should reputation metrics be shown? The answer depends on the application scenarios, such as the ones developed in *PrimeLife* Activity 1. For instance, in the MediaWiki application scenario of Work Package 1.1, if a user looks up an article, the reputation metrics of the authors of that article should be displayed as well.

# Chapter 5

# User-Friendly Policy Management and Presentation

This Chapter summarises some of *PrimeLife*'s WP4.3 main research results within the first project year. WP4.3 work has addressed both simplified means for users to define, adapt and administrate data release policies (i.e., their privacy preferences, or as we say in short: their "PrivPrefs"). Besides, it has been addressed how the services side's data handling policies and their correspondence to the user's PrivPrefs can be presented in a user-friendly manner.

## 5.1 The Privacy Preferences Concept

The concept of Privacy Preferences (PrivPrefs) is introduced in [Ber08, FHPB+09]. To recall:

> PrivPrefs represent certain privacy preferences a user applies regarding a dedicated Service Provider (SP) for a dedicated purpose. A PrivPref contains the acceptance of a *dedicated purposes* for a dedicated *SP*. Additionally it could contain statements about the acceptance of disclosure of *additional data items* for the contact and only for this purpose. Furthermore they contain statements on user-controlled linkability of different actions.

A PrivPref is used to **match** (i.e. compare) **the SP's**[1] **privacy policy with the privacy preferences** the user (Service Requester (SR)[2]) has expressed beforehand. In this context a **privacy policy** represents a collection of non-negotiable, concrete privacy-related statements about the service provider. We assume that a valid privacy policy contains statements about the requested data items, the purpose of the data request, and the data controller itself. The research in the field of privacy policies, expression,

[1] We use contact and SP synonymous
[2] We use user and SR synonymous

automatic negotiation, etc. is out of scope of this document. A PrivPref data structure can be noted as shown in Listing 5.1.

```
1  enum PrivPrefType {TypeA, TypeB, TypeC};  // defines PrivPref Types:
2                                            // A - anonymous
3                                            // B - necessary PII
4                                            // C - additional data
5  class PrivPref{
6     PrivPrefType    type=TypeA;      // contains the concrete type, default is A
7     URI             contact;         // contains the unique Id of the contact
8     URI             purpose;         // contains the unique Id of the purpose
9     DataTypes[]     addData;         // contains a list of accepted add. data
10    Boolean         linkable=false;  // contains true or false, default is false
11 }
```

**Listing 5.1**: Schematic data structure of a PrivPref

User tests showed that users do often not alter the default settings [AR97]. Besides users often do not understand the complex security and privacy mechanisms. Therefore we have to support them by offering useful default settings for their privacy preferences regarding the amount of data to disclose, regarding the necessity of the data and desired linkability of transactions, etc. These default settings, represented by our PrivPref types (see item PrivPrefType in Listing 5.1), do not contain concrete values for contact and purpose, but define default privacy preferences, like anonymity, amount of data and linkability of certain user actions. The PrivPref types, listed below, could be seen as templates of all derived PrivPrefs. The instances of the templates contain some specific preferences, the user assigned during data disclosure. Usually these preferences are dedicated values for contact and purpose and, in case additional data are disclosed, the amount of additional data the user *accepted* to disclose. We define the following PrivPref types to assist the user to start with:

a) *Anonymous, no Personally Identifiable Information (PII):* This type of PrivPref applies the strongest privacy protection. It does not allow any data disclosure. Only a transaction pseudonym is revealed. Optionally, the user can decide on linkability to former actions.

b) *Identifiable, only necessary*[3] *PII:* This type of PrivPref provides a moderate level of privacy protection. It allows to disclose only necessary PII regarding a dedicated purpose, thus serving the data minimization privacy principles. Usually these actions are linkable by design if the user reveals identifying data items[4].

c) *Identifiable and additional PII:* This type of PrivPref offers the weakest level of privacy protection. It allows disclosure of additional PII, not really necessary for the dedicated purpose.

[3]The necessity of data for a certain purpose is defined by a trustworthy organization. The user is allowed to add exceptions per contact. In this case also type b) PrivPrefs contain additional data. The difference regarding c) is explained below in Section 5.3.

[4]For simplicity we assume that PII makes identifiable. However linkability computation is another research area [Cla07].

Usually we start with maximum privacy - that means PrivPref type *a*) is used as template for new PrivPrefs for new contacts. If a statement in the privacy policy and the corresponding PrivPref does not match, e.g. if the SP requests PII for a purpose that the SR has not agreed upon or if the SP requests more data than needed for the purpose etc., the system displays warnings, corresponding to the mismatch(es) (see Section 5.5). Therefore, using these PrivPref types, we enable the user to manage data disclosures in a more privacy-friendly manner because PrivPrefs structure the data disclosure process. Besides PrivPrefs do inform and guide the user to detect and to solve mismatches of privacy policy and privacy preferences in a non-intrusive way. In the following, we will discuss the concept behind PrivPrefs in more detail.

## 5.2 Parameters of the PrivPrefs

Based on the PrivPrefs definitions above and for enforcing privacy principles such as data minimization and purpose binding as stated by [Cou95], we define three main parameters *Contact, Purpose and Data* that are determining the user's privacy preferences.

1) We for simplicity assume that all *Contacts* in our work can be identified by URIs (Unified Resource Identifier (URI)). These are unique addresses, indicating the contact. Due to the lack of a consistent name schema we use the ordinary Internet domain of the SP. However they could be replaced by URIs later on. Well known contacts are google.com, amazon.com, ebay.com, wikipedia.org etc.

2) *Purposes* are represented by URIs, defined by an external trustworthy organization (e.g. World Wide Web Consortium (W3C), etc.) and express the purpose why a certain data item is requested. Typical purposes could be *Registration, Authentication, Order, Shipping, Payment, Search, Blogging* etc. Each purpose has assigned a well defined *set of data types* which are needed by the SP for achieving this purpose. The data types are not content of the PrivPref. They are defined per purpose by a trustworthy organization. The user is allowed to define his own data sets.

3) *Data items* are categorized (address, name, zip-code, pwd, date of birth etc.). An ontology, released by an external trustworthy organization (e.g., Independent Center for Privacy Protection, Schleswig Holstein, Germany (ICPP), W3C), may be applied for that.

4) *Additional Data* are data not really necessary for a certain purpose. The definition, which data items are needed for what purpose, is done by an external trustworthy organization (W3C, ICPP, etc.). The user has to explicitly accept these additional data items.

PrivPrefs aim to assist the user in selecting the right data items for a service provider. Based on the current PrivPref setting for this context the system suggests corresponding data items, fulfilling the data request.

## 5.3 PrivPref Configuration

The PrivPrefs represent an essential building block of our user-friendly approach for informing the user about the implications of the privacy policies of the services-side. In the following, we will elaborate the configuration of the PrivPrefs and the management respectively the assignments of the PrivPrefs for a certain contact during transaction. We introduce some axiom-like rules for PrivPref handling. We define some fundamental rules regarding PrivPrefs:

1. Every dialogue starts with the preferences, derived from PrivPref type *a*) as default, i.e. with maximum privacy.

2. The pre-defined PrivPrefs are not changeable. They are templates for all derived and are used to specify the types of the new PrivPrefs based on their types.

3. There is no possibility for double PrivPrefs. A PrivPref is addressing exact one *Contact/Purpose* pair. Also each pair of *Contact* and *Purpose* is exactly addressing one PrivPref.

4. The user may use another PrivPref b) or c) for a certain data disclosure. If additional data are requested by the SP, there are two options. Either the user selects the PrivPref c) and therefore allows the disclosure of additional data for this contact[5] or the user allows the usage of exactly the requested data items. The first option expresses a higher confidence in the contact's rightful behaviour as it sets preferences that are valid also for further data requests during that transaction whilst the latter represents some pragmatic and more privacy-concerned approach.

5. To support the user in making the right decision regarding the selection of a suitable PrivPref for a certain transaction, we suggest to select the PrivPref b) per default, even if additional data are requested. This assures that the user is warned in case the same contact requests further additional data for the same purpose. As far as the user usually accepts the default options [Nie04], we propose the more privacy-friendly setting per default. However, the user is able to change this setting to PrivPref c) as shown below in Table 7, Line 4.

6. If the user already has a PrivPref defined for a certain purpose and contact, the system will automatically select the corresponding PrivPref. The warnings will be adapted accordingly. If during this kind of request additional data are not permitted by this PrivPref, the user will be informed as usual. The user is offered two options – to extend the existing PrivPref or not to store the current setting.

7. For PrivPref a) no linkability is set per default. If PrivPref b) or c) are assigned, all user actions can be linked (as stated in the PrivPref description). Additionally, the user can *explicitly* link two actions together. However an automatic linkability computation on the user-side, based on user data disclosed, in order to inform the

[5]That means, the user will not be warned any more, if the contact requests further additional data. This does not mean the contact gets a general permission to access additional data. It just suppresses the warnings. The question regarding consent to the disclosure of the additional data items is presented anyway.

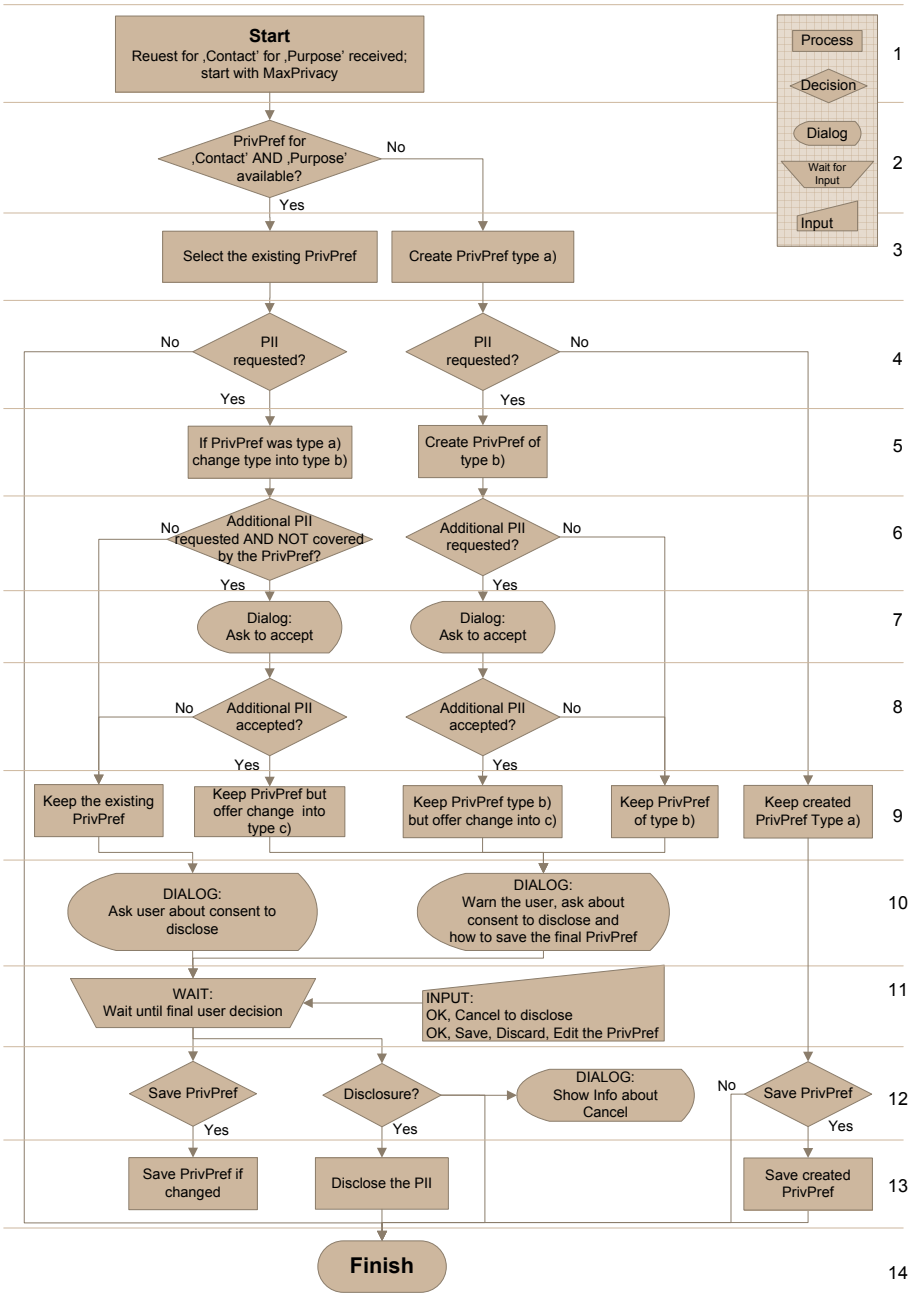



**Figure 22**: PrivPref Configuration Walkthrough

user about privacy risks, is too complex [Cla07] and thus not considered by our approach.

| Step | Description |
|---|---|
| 1 | The user visits a web site. The contact partner, identified by an URI requests some data for a certain purpose. |
| 2 | A check regarding a PrivPref for the contact and purpose is performed. |
| 3 | If a corresponding PrivPref is found the preferences are taken for further elaboration. If there does not exist an appropriate one for this combination of contact and purpose, we have to create a new PrivPref based on template a). |
| 4 | To decide about how to proceed, we have to consider about the requested PII. |
| 5 | If an appropriate PrivPref was found and it was of type a), we change the type to b), because PII are involved. In case no PrivPref was found (in step 2), we create a PrivPref of type b). |
| 6 | In case that we have found a suiting PrivPref so far, check if the disclosure of additional data are requested but NOT covered by the existing PrivPref. In case that no PrivPref is available, check whether additional data are requested or not. |
| 7 | If additional data are requested (but not covered in case of an existing PrivPref), ask for confirmation to disclose also the additional data. This also handles the case where a SP requests various optional data where the user is willing to disclose only few of them. |
| 8 | Check if the disclosure of (any) additional data were accepted. |
| 9 | Perform the 'final' consolidation regarding the selected PrivPref for all further activities. In case there is an existing PrivPref and there was no PII requested, just keep the PrivPref, selected in Step 3 respectively Step 5. If additional data are involved and accepted, then the user may change the existing PrivPref towards PrivPref type c) in the next step. If no PrivPref available, two cases to distinguish. If no additional data are accepted at step 8, keep the type of the PrivPref, if additional data are accepted, offer additionally to change the type to c). If no PII was requested and new PrivPref type a) was created, we just proceed (to Step 12). |
| 10 | In case the existing, PrivPref is kept, the user is asked to confirm the disclosure, as shown in Figure 25. In case there are changes, the user is warned respectively informed about these changes and asked to confirm or correct the pre-selection, made in the steps before. A typical dialogue could look like shown in Figure 25(a) or Figure 28. |
| 11 | Wait until the final decision of the user. Possible decisions could be to perform or to cancel the disclosure and to save, edit or discard the proposed PrivPref. |
| 12 | Check whether to save or not to save the PrivPref if changed. Check whether to perform or to cancel the disclosure. In case of cancelling the disclosure, the user is informed accordingly. |
| 13 | Save the current PrivPref (Type of PrivPref, contact URI, purpose URI, additional data disclosed and selected linkability). The PrivPref gets persistent. Finally disclose the PII. |

| Step | Description |
|---|---|
| 14 | The process of data disclosure and PrivPref configuration is finished. |

Table 5: PrivPref Flowchart Description

The flowchart of the configuration of a PrivPref during the process of data disclosure is shown schematic in Figure 22. The corresponding description is listed in Table 5. We have to differentiate between "create" and "save". The first creates a new, temporary PrivPref. If the user cancels the action, the PrivPref is discard. The latter saves the PrivPref persistent and makes it available for further use.

## 5.4 PrivPref Application

In the following we apply the PrivPref approach in a possible example scenario. We observe a user who is visiting the bank, checking email, accessing a social network, performing search and contributing to blogs. For demonstration purpose we define the necessary purposes and the type of data associated to the purpose in Table 6. This table in real should be issued by a trusted organization, like ICPP, W3C or a customer organizations, etc.

| Purpose | Necessary data |
|---|---|
| ebanking | AccountN$^{o}$, Password, FullName, Date, eMail |
| email | Email, Password |
| search | SearchQuery(any term(s)) |
| blog | NickName, Password, Text |
| network | UserName, Password, Text |

Table 6: Our makeshift purpose definition

| Time | Action | Action Details | PrivPref[6] and Warning |
|---|---|---|---|
| 1 | Visit a bank account | page='cash.bank.com',<br>URI='bank.com',<br>purpose='ebanking' | new PrivPref,<br>$P1_b = (bank.com, ebanking)$<br>Warning about **new contact and new purpose**. |
| 2 | Email account access, date of birth is requested additionally to verify age. | page='mail.global.com',<br>URI='global.com',<br>purpose='email',<br>additional='Date' | new PrivPref,<br>$P2_b = (global.com, email, Date)$<br>Warning about **new contact, new purpose and additional data**, PrivPref saved. |
| 3 | Other email account, same PII as above, at the same service. | page='mail.global.com',<br>URI='global.com',<br>purpose='email',<br>additional='Date' | use existing $P2_b$<br>No warning, because **PrivPref fits**. |

| Time | Action | Action Details | PrivPref[6] and Warning |
|---|---|---|---|
| 4 | Social network, various PII requested to present the career (CV). | page='net.work.com', URI='work.com', purpose='network', additional='CV' | new PrivPref, $P3_c = (work.com, network, CV)$ Warning about **new contact, new purpose and additional data**. User selects explicitly type c) for convenience. |
| 5 | Other email account, different provider, no additional data. | page='mail.local.com', URI='local.com', purpose='email' | new $P4_b = (yuhuu.com, search)$ Warning because **new contact**. |
| 6 | Use a search engine | page='search.global.com', URI='global.com', purpose='search' | new PrivPref, $P5_a = (global.com, search)$ Warning about **new purpose**. |
| 7 | Use a map service, perform a search for a location | page='maps.global.com', URI='global.com', purpose='search' | use existing $P5_a$ No warnings, because **PrivPref fits**. |
| 8 | Use another search engine | page='www.yuhuu.com', URI='yuhuu.com', purpose='search' | new PrivPref, $P6_a = (yuhuu.com, search)$ Warning, because **new contact**. |
| 9 | Blog at a certain blog forum, date of birth for age verification requested | page='www.blog.com/drugs', URI='blog.com', purpose='blog', additional='Date' | new PrivPref, $P7_b = (blog.com, blog, Date)$ Warning about **new contact, new purpose and additional data**, PrivPref not saved. |
| 10 | Blog at another blog forum, no additional data requested | page='www.blog.com/books', URI='blog.com', purpose='blog' | new PrivPref, $P7_b = (blog.com, blog)$ Warning, because **no PrivPref found**, **new contact, new purpose**, PrivPref not saved. |
| 11 | Returning to the bank | page='cash.bank.com', URI='bank.com', purpose='ebanking' | use $P1_b$ No warning, because **PrivPref fits**. |
| 12 | Returning to the social network, other PII requested to present the education. | page='net.work.com', URI='work.com', purpose='network', additional='Education' | use $P3_c$ No warning, because **PrivPref fits**. |

Table 7: Evolution of the PrivPrefs

Table 7 shows that our PrivPref approach is applicable in usual online scenarios. However, as demonstrated in line 9 and 10 it may be insufficient to use the domain address as contact URI because two possibly different blogs are assumed as belonging to the same contact. This underlines the requirement to enhance the communication protocol between client and server to transfer contact URI, purpose of the data request, requested data types, etc., as proposed in the *PRIME* project [SMP08].

[6] We use the following notation: $Pn_t = \{contact, purpose, data_{add}\}$ where P stands for PrivPref, n is the number of the PrivPref, t denotes the parent PrivPref a, b or c. and $data_{add}$ lists the additional data items

## 5.5 Presentation of Matches and Mismatches of PrivPrefs and Privacy Policies

There are principally untold possibilities to visualize the fact of a mismatch. During the pilot tests for PRIME Integrated Prototype Version 3 (IPV3) we found out that users get confused about obtrusive warnings and that they finally switch off all the protection and warning mechanisms [Lin08]. Therefore we suggest to shift the character of privacy related message from interfering warning towards information. Instead of a red exclamation mark we could use a information cloud as a metaphor for instance. Different types of clouds like fair-weather cloud, rain cloud, thunder could etc. could help to inform but not frighten the user. In the following we propose three different approaches to present the privacy-related information and to visualize possible mismatches between privacy preferences of the user and the privacy policy, stated by the service provider.

We elaborate a static, a dynamic and a mixture–of–both presentation approach and discuss the benefits and drawbacks.

### 5.5.1 Static Presentation Approach

In the following we present an example, how the presentation of the privacy policies and their correspondence with PrivPrefs could look like using static user interface elements. We motivate the proposal and discuss the benefits and drawbacks.

Figure 23 shows an example dialogue similar to a well-known online service requesting user name and password for authentication. We will use this scenario to discuss all following proposals. All proposed colour schemes and labels in the interfaces are subject to further research and tests and represent some kind of place holders until better solutions are found. In recent literature [WMG06, MC04, Ben98, AR97] we found some

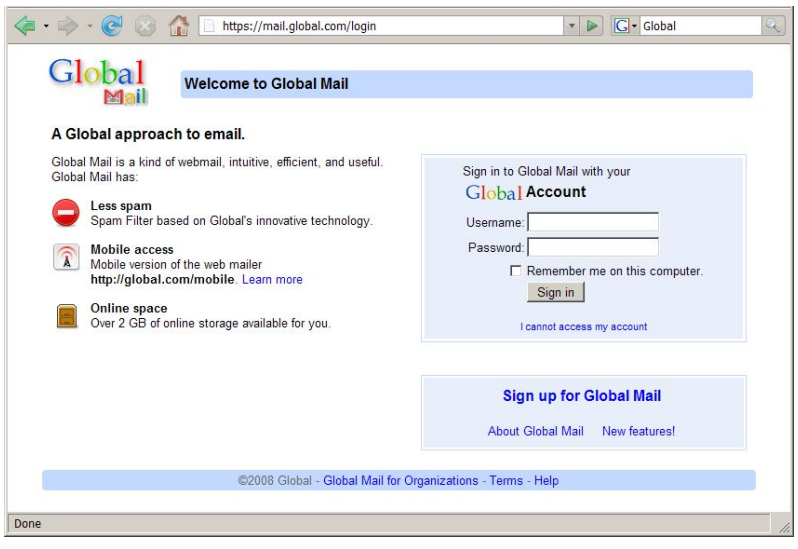



**Figure 23**: A conventional interface for online services for authentication

influencing factors regarding privacy:

1. Privacy is usually not the primary intend. Therefore privacy information has to be less prominent and supporting the user in performing the primary task.

2. Information, not really belonging to the primary task, is perceived very weak. So privacy-related information has to be placed nearby the affected data item.

3. The policy-reading behaviour of the normal users is weak, that means the ordinary user does not read the privacy policies. We have to present the major facts of the privacy policy in such manner that the user may read it without being forced to perform additional interaction.

4. Users are very sceptical regarding interface elements, similar to advertisement banners. Textual information is often more appreciated. Therefore we have to design the approach to present the information about the privacy policy and the (potential mis)match very restrained.

5. User do often no alter the default settings. Therefore we have to offer privacy-friendly default settings bearing the issues above.

We start with a static approach, using a title bar alike line on top of the ordinary input fields. We call it 'Privacy Bar' or just 'Bar' in the following. The bar allows us to visualize the privacy policy items and to offer PrivPref management capabilities. If the user moves the pointing device (mouse) over one of the text fields (hovers), the corresponding short information of the privacy-policy respectively some PrivPref-management capabilities are provided automatically. An user survey showed that the user perceives these kind of additional privacy-related information [Ber09]. This solution offers short privacy-policy


(a) Contact mismatch

(b) Purpose mismatch

**Figure 24**: Static interfaces I

information just at fingertip without requiring any additional mouse click. The user gets a rough overview about the three major components of the data disclosure – to whom to send which data for which purpose. This guarantees that the privacy situation does not become worse applying this interface than today's interfaces using (or not using) the ordinary privacy-policy link at the bottom of the web pages. In our proposal the user gets offered additional information. If the user ignores this additional information, the level of information at least corresponds to the situation without the privacy bar.

Figure 24(a) shows the case a user is visiting a new contact. The whole bar is coloured[7]. If the user moves over one of the three presented items, more detailed information regarding a short privacy notice is shown. Some prominent text explains the situation. In the example some red text is shown to attract attention to the fact of the new contact. A button is provided to add the contact to the user's list of known contacts. However, the control element can also be implemented as link, checkbox, dropdown list etc. Using this control element, the user is able to store dedicated privacy-relevant information. The visualization is adopted accordingly. In this case the background colour of the contact area in the bar is reset to normal, the additional control elements are altered to offer undo capabilities.

If the user uses the 'Keep?' link, contact, purpose and configuration regarding additional data are stored at once to adapt the PrivPref as described above. The visualization is adopted accordingly. That means no more warnings are displayed, additional control elements offer undo capabilities. If additional data are requested, a warning message may be presented. However such warning messages are usually ignored [ECH08], so we tend to rather inform the user less intrusively.

The situation, a user visits a known contact but for an unknown purpose, is shown in Figure 24(b). The structure of the interface elements is similar to the structure for new contacts. The short privacy policy informs about purpose details of the privacy policy of the SP. The user may accept this purpose for the current contact. This effects that the visualization of the mismatch is rest to normal, the additional control elements are altered to offer undo capabilities. In case, additional data are requested, we alter the


(a) Additional data requested

(b) No mismatch, some details

**Figure 25**: Static interfaces II

structure of the interface a bit as shown in Figure 25(a). Each additional data item gets assigned a control element to accept the concrete data element for disclosure. If the user accepts a certain data item for disclosure the corresponding control element is altered to offer undo capabilities. If the user wants to assign the PrivPref *c*) to this setting, he has to use the PrivPref Manager, available via the right-most icon for PrivPref management, sketched in Section 5.5.4. This will alter the underlying PrivPref.

Figure 25(b) shows an example, where no mismatch occurred. The interface just informs the user and offers a decent appearance. The 'Keep?' link is missing because there are no settings to keep. If he user wants to manage the affected PrivPref, the

[7] As noticed, which colour – red or yellow or similar to achieve an appropriate warning effect is subject of further research and tests.

PrivPref management is accessible via the icon on the right side.

The texts, icons, colours etc. in the mock-ups are just for illustration and should be elaborated and tested further. E.g. an alternative text for the 'Keep?' link could be for instance "store" or "save".

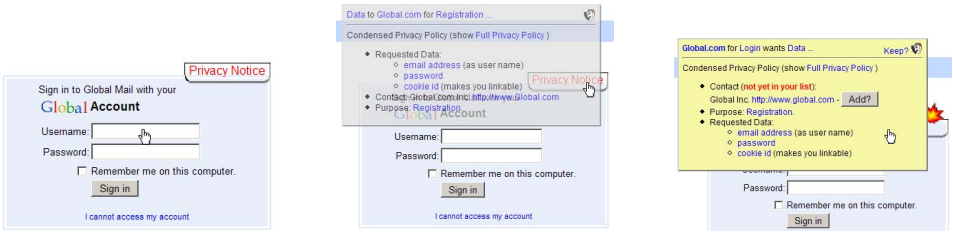
One drawback of this static approach is that it is invasive with regards to the original web site. This means, the original web site layout will be altered in few details. This may discourage SPs in using this technology, because it may ruin the original interface. Besides, the user may just overlook it because of the decent and restrained presentation mode. Using colours and font sizing methods may compensate this effect but boosts the invasive effect of the interface. To enable colour-blind people some intuitively understood icons or symbols could be used. However this boosts the invasive effect even more.

### 5.5.2 Dynamic Presentation Approach

The static approach, presented above got promising results in a user survey [Ber09]. However one of the major drawbacks of this design already mentioned above is that it deranges the original web site design and hence may get less support from the SPs than a less invasive approach. An dynamic approach, were the information appears on demand like tooltips do, may be a better solution.

We developed an interface where a control element, offering information about the services side's privacy policy, appears when the user enters a certain area with the pointing device (mouse) or when a control element inside this area gets the input focus.

Figure 26 shows the idea behind the dynamic approach of the privacy-enhancing user interface. If no user action is performed within a certain area of the input fields our control element is hidden (see Figure 23). The additional control element does not occur until the user moves the cursor into the data input area, as shown in Figure 26(a). The usage of the interface is organized in two steps. At a first step only the button-




(a) Interface visible because mouse hovers the form

(b) Details visible because mouse hovers the control element

(c) Mismatch example: Contact not yet known

**Figure 26**: Dynamic interfaces

like element appears. Using different colours and expressive icons we may illustrate some general properties regarding the matching or mismatching of the privacy policy and the PrivPref. We may use colours and icons to visualize the different states of match respectively mismatch. If the user is accessing the web page of a new contact, the system could use a more prominent presentation. An example is given in Figure

26(c). If the user wants more information, he just moves the cursor into the control element area. Using the hover effect we are able to present privacy-related information on different levels to the user without any additional click. The setting could be kept by clicking one of the offered links in the second level interface, as shown in Figure 26(b). The transparent background of the information panel is used just for documentation. In our tested prototypes the background of the panel is opaque. However transparency could be used as a further design element too. The usage and meaning of the interface elements are analog to the static approach, explained above. The text and the icons of our current prototype are our first proposals and should be elaborated and tested further. Alternative text for the control element could be for instance "Privacy Info", "Privacy Policy" etc.

Besides the benefit not to alter the original interface we see the benefit that the sudden occurrence of the control elements helps to attract the users' attention. A first pilot test, performed within the *PrimeLife* project, showed that users do perceive the dynamic approach much better than the static one [KW09]. However the user test also indicated that users may perceive the static approach as more trustworthy than the dynamic approach. This may be due to some kind of similarity to advertisement elements. Further user tests should elaborate the details in depth. A further drawback is that the user interface of the first step (Figure 26(a)) has only a limited information capacity to inform the user about the major privacy-related facts. A combination of both interfaces could help here. We will present this approach below.

### 5.5.3 Hybrid Presentation Approach

To take the advantages of both of the presented approaches and to overcome their drawbacks we propose to combine both approaches. The privacy bar should only occur, if the user really needs it. It keeps the original interface unchanged and gathers the user attention because of the dynamics. Besides it offers some idea to the user about the match or mismatch of privacy policy of the SP and the user's privacy preferences. Besides, it even allows to access the short privacy policy without any additional click. The user could proceed as usual after he had read the privacy policy. Figure 27 presents corresponding examples. Figure 27(b) shows the appearance of the privacy bar similar to the static version, presented in Section 5.5.1. If the user moves the mouse over the input area of the dialogue this privacy bar occurs, containing the same elements as the proposed static version. However the bar contains one additional element, symbolizing a drop-down capability. If the user hovers this element with the mouse (no click is necessary), a panel is shown with details about the condensed privacy policy of the service provider, further helpful details for the user and a link to the full privacy policy. In our example at Figure 27(b) we show the case of a not yet known contact.

One of the benefits of this interface approach is that the original user interface is not changed at all. The control elements are laid on top (like overlay) of the original interface and therefore cover the underlying elements. Another benefit is that we are much more flexible in designing appropriate appearance models for the control element because we are not mentally bound to the original user interface any more. Further user tests have to elaborate the proposal and their variants in detail.


(a) First step, privacy bar visible

(b) Second step, details visible

**Figure 27**: Hybrid interface proposal

### 5.5.4 A Proposal for a PrivPref Management UI

The PrivPref management User Interface (UI) is accessible via the right-most icon in the privacy bar. We also use the hover effect to display this interface. Alternatively we could show the interface, if the user clicks on the icon. We decided to use the hover effect to minimize the number of necessary clicks for the user to access the desired functionality and to minimize the interference for the user. To fulfil the essential usability requirement "simplicity" we keep the functionality of the PrivPref Manager (PPM) very limited. The PPM has to present the existing properties in context of the disclosure. The presentation of all existing PrivPrefs may be accessible via an additional control element, but is not shown in our example. It could be realized as list or tree view with all contacts (including the related addresses), the assigned purposes and possible additional data. Filter mechanisms may allow the experienced user to cluster the existing information to look for dedicated facts.


**Figure 28**: The PrivPref Manager User Interface Mock-up

The PPM user interface consists of two sections. The upper part is the informational part, were information about the current disclosure is shown. It may also contain additional control elements to manipulate single items, like contact, data items etc. separately. However for simplicity we did not use such elements in our example. The lower part offers functionality to select and assign an appropriate PrivPref. Figure 28 shows a simple mock-up of a PPM user interface.

## 5.6 Open Issues

The above sketched interface proposals should help the user in managing PII disclosures. However, there are still some open issues and questions requiring further research:

- How to mark optional/mandatory data items?
- How to deal with "many" purposes in one form or web site?
- How shall we treat user-generated text (e.g. blog or forum entries) and multi-media content (e.g. photos, audio or video snippet)? Should we store them, because they can become PII? How to classify these data items in the set of purpose and data item?
- As mentioned above, a contact is identified by his URI. However, this id is often not available for a SP. Besides it may make sense to take also a service identifier into account to be able to differentiate between different services of one service provider. Google Mail and Google search may be an example.

# Chapter 6

# Conclusions and Outlook

Privacy-enhancing IDM will only be used if it is usable. *PrimeLife* Activity 4 (HCI) is therefore conducting research on intuitive and usable user interfaces for *PrimeLife* technology which are also fulfilling legal and social requirements. In this first version of the *PrimeLife* HCI Research Report, we present the most important research contributions of *PrimeLife* HCI Activity.

These contributions comprise new methods and success criteria for evaluating PETs such as for instance the CURE virtual usability laboratory for asynchronous on-line user testing of small prototypes of PET solutions and the PET-USES which is being developed in order to measure the usability of privacy related aspects of UIs. As PETs include a verity of functionality the PET-USES is modular insofar that it is constructed of several sub-scales relating to specific PET functionality and thus can be adapted to a wide range of applications.

The research report also comprises first work on the mental model of credential selection and anonymous credential selection mock-ups. The multi faceted problem of users neither understanding the problem (i.e. why and how to achieve data-minimisation in on-line transactions) nor the possible solution (i.e. with a local client that holds anonymous credentials) is proving to be equally as challenging as interesting. This problem is also related to the challenge of mediating reliable trustworthiness of communication partners to end users. Former studies conducted within the *PRIME* project showed that users often do not trust the claims that PETs can really protect their privacy and that many users have great trouble in differentiating between user and services sides. And, accordingly, users believed that the assurance evaluation was an evaluation of their and not the recipient part of the transaction. As the results of our HCI work for a trust evaluation function show that these problems can at least be alleviated by combining several UI concepts, this approach will be used in the coming credential selection studies.

Furthermore the first version of the *PrimeLife* HCI Research Report includes new approaches for configuring privacy preferences "on the fly" and for presenting policies and their (mis-)matches with the user's preferences in an informative, understandable, legally compliant and non (or at least not overly) interfering manner.

Most of the HCI research work presented in this report is work in progress. In

particular, the UI concepts and mock-ups presented in Chapters 3 to 5 need to be further tested and subsequently elaborated. In its future work, the *PrimeLife* HCI Activity will also put more emphasis on research of usable and legally compliant transparency and policy tools for virtual community users, based on the legal aspects for virtual community applications that are currently analysed by the *PrimeLife* ULD and needed for prototypes in Activity 1.

Chapter A

# PET-USES 1.0

**PET-USES[1.0]**

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 indicate to what extent you disagree or agree to the statements below.

| | *Completely disagree* | | | | | | *Completely agree* |
|---|---|---|---|---|---|---|---|
| I found it easy to learn how to use the *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I had to learn a lot in order to use the *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I keep forgetting how to do things with this *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I often have to look at the instructions wile using the *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I need a lot of assistance to use this *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find the *system* interface easy to use | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find the organisation of the *system* interface understandable | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I get confused by the *system* interface | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find it very difficult to work with the *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find it easy to get the *system* to what I want | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find that the benefits of using the *system* are bigger then the effort of using it | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would like to use this *system* regularly | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find the functions offered by the *system* appealing | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| The *system* makes it easy to decide if it is safe to release my data | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I think this *system* makes it easier to manage my personal data | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I feel safer releasing my personal data when the *system* states it's ok | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I get a clear view of my personal *data* from the system | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find organising my personal *data* easy with this system | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find keeping track of various user names and passwords becomes easier with this *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find it easy to add personally issued credentials into the *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find it easy to add / import certificates into the *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find it easy to use settings for how much or how little *data* to be released | | | | | | | |
| I find that the *system* helps me understand the effects of different privacy settings | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I feel safer knowing that I will be notified if I'm about to release more *data* then my chosen preference | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I get help from the system to evaluate the trustworthiness of the *data* recipient | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I don't understand how the *system* determines if a data recipient is trustworthy | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I get help from the system to understand who will receive my *data* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I now know when I'm releasing personal information | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I know what personal information I'm releasing | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I find it easy to decide how much or how little *data* to release in a given transaction | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I can easily find out who has received my personal *data* with this *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I get a good view of who knows what about me from this *system* | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I can easily see how much I've used a particular username with this system | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Chapter B

# *PrimeLife* Personas

PrimeLife

# The PRIMELife Personas

Authors

Christina Köffel (koeffel@cure.at)
Erik Wästlund (Erik.Wastlund@kau.se)
Peter Wolkerstorfer (wolkerstorfer@cure.at)

Persona drawings
Sandra Dittenberger (dittenberger@cure.at)

March 2008

Contact

CURE
Center for Usability Research & Engineering
Hauffgasse 3-5
A-1110 Wien
Austria

Tel: +43/1/743 54 51-46
Fax: +43/1/743 54 51-30

# Content

# 1 Introduction

This paper collects the personas developed for the PrimeLife project. We show why we use personas in PRIMELife and deliver their description.

In the task description of task 4.1.1 (page 81, Annex I “Description of work”) we promise that:

> *The results of this task feed directly into the other tasks in this work package and* ***ensure a strong focus on the user*** *throughout the project.*

To achieve the goal of “a strong focus on the user throughout the project” we have decided to use the personas method.

## The Personas Method

Alan Cooper [Cooper, 1999] - "inventor" of the personas-method describes it like this:

> "*Personas are not real people, but they represent them throughout the design process. They are hypothetical archetypes of actual users. Although they are imaginary, they are defined with significant rigor and precision.* "

In general personas show the scope and nature of the design problem. Until “the user” is precisely defined, we can always imagine that we ourselves are the users [Pruitt and Adlin, 2005]. We have different pictures in mind which hinder fluent communication:

Personas as communication tool allow defining which users we are building for and synchronize the pictures in our minds:

"*We are social mammals whose brains are highly specialized for thinking about others. Understanding what others are up to--what they know and want, what they are doing and planning--has been so crucial to the survival of our species that our brains have developed an obsession with all things human.*

*We think about people and their intentions; talk about them; look for and remember them.*" [Gilbert 2006]

A lot of companies (**Microsoft** [Pruitt and Grudin, 2003], Ford, Chrysler, Sovereign Bank, Amazon, Best Buy, Staples, FedEx, UPS, **IBM**, **SAP**, SONY, Razorfish, Pfaltzgraff, Yahoo! Media, Electrolux, Cisco [Nieters et al, 2007]) use personas successfully because of their advantages - which are:

1. Support having the **same picture** of our end-users in mind for everybody in the project; hence reduce communication-complexity which makes communication easier and more fluent (this again saves time explaining "the user" every time he/she appears in a communication process).
2. Bias the minds of everybody in the project towards **user-centred thinking**. This gives the otherwise "technical touch" of R&D projects a humane touch and brings things to live in a natural way (as human minds deal great with other persons – but human minds have a hard time when dealing with abstract big bunches of data) – personas make use of the "Emotional Mind" of people [Shyba and Tam, 2005].
3. Be an **evaluation tool** as walkthroughs can be conducted with personas (which is very handy to judge design alternatives).
4. **Leave** the world of **possibility thinking** as you never fall back to „the user".
5. They can **shorten feature debates** which saves time.
6. A tool to help the whole project team **focus on the needs** of our target **users** instead of using a different ad hoc "the user" definition which comes to mind at a point in time (Humans have just one locus of attention. It lies in the nature of R&D that the developers' locus of attention is focused on the technical issues and not the real end-users. Therefore there is a need for methods solving this missing focus on the end-user. Personas are one way to do it).
7. Unobtrusive - the do not modify any existing processes and unfold their power subtly in the minds of people; they make thinking about "the user" **more convenient.**
8. Unlike bunches of data personas support **informed design** (you can design UIs for persons – not for data representations).
9. According to Cooper the design process becomes **„enlightened".**

## *Next Steps*

The next step is to evaluate the personas [McGinn and Kotamraju, 2008] with the help of the consortium partners. After that a personas campaign will be started with a kick-off to introduce the personas to the whole team and explain their usage.

## *Using Personas*

The personas will be kicked-off in the meeting at Stockholm.

The basic requirements from the consortium partners by now are:

1. **Instead** of talking about **"the user"** (e.g. scenarios, discussions, descriptions…) one fitting **persona name** (if two personas fit just decide for one which fits slightly better) should be chosen; if there is no fitting persona request a new persona from CURE.
2. The **persona representations** (which will be delivered by CURE) should be **present** in the development team (e.g. by pinning their descriptions on the walls of the development room).

# 2 The PRIMELife Personas

## *Inga Vainstein*

46 years/ female/ Sweden

"In my job everything depends on my reputation."

| | |
|---|---|
| **Date of Birth** | 21st December 1962 |
| **Description** | Inga is 46 years old and is currently working as journalist. As a part of her job she is travelling to various countries. She is very anxious to keep her public profile clean in order to have a good reputation and to appear trustworthy. Inga likes to take pictures of sights in every city she has been to. A few years ago she bought professional digital photo equipment. |
| **Social Situation** | Inga was married once but got divorced 8 years ago. Since then she is single and likes dating. Inga does not have children. |
| **Health Situation** | With her growing age, travelling and the stress in connection with the journeys start to become a problem for her. |
| **Financial Situation** | Inga is free of debts and her salary is situated in the higher middle-class. |
| **Technological Knowledge and Usage of Technology** | Inga is using mobile phones since 12 years (she regularly switches provider and phone). She uses her phone mostly to make calls and write messages. Furthermore she likes having her electronic calendar always with her. She has her own laptop for writing her articles. Inga uses common office and e-mail tools on a daily basis. Since she is a fan of photography and recently started to provide the pictures for her articles, she knows some photo editing tools. Although Inga is using computers regularly for work and leisure purposes, she is still insecure and afraid of problems that might occur. |

**Web- usage**

Inga uses the internet on a daily basis for private as well as professional purposes.
What she does online:

- Photo- blogging of her trips
- Shopping (clothes & camera equipment)
- Audio and video conferences
- Community networking (social networks, online forums)
- Dating-services
- Collaborative Workspace

Inga uses mobile internet and diverse wireless connections when she is on a business trip. At home she has a broadband connection.

**Negative Experiences**

Friends posted party pictures of her being drunk at a costume party and linked them to her, which resulted in a bad reputation at a job interview.
Sometimes Inga can't cope with the amount of SPAM mails she gets.
Once Inga lost a USB stick with important data (articles she was working on) during a trip.

**Wish list**

Inga hates it when she has the feeling that the system controls her. She wants to decide who is able to see and use her data. She frequently googles herself to keep track of what data is publicly available about her.
Inga doesn't want that private information such as her dating profile becomes public. Therefore she uses a pseudonym on such sites.
Since her reputation is important to her, Inga does not want her colleagues to find out that she orders her clothes in mail-order companies.
Generally Inga wants her (private and professional) data to be safe and separated. She does not have a lot of time to spend on security. Inga has tried to use security software to keep her data safe, but it was too complicated for her. At the beginning she was reading almost every pop-up message. After a while she got frustrated because she did not understand the information provided and since then most of the time she just clicks okay to make the pop-ups disappear.

**Additional Information**

Inga likes to use free wireless hotspots at airports which are not encrypted most of the time. She is afraid that somebody might fetch her passwords, still being online is more important than these concerns.
Inga does some of her shopping online. When she is looking for special items, she has to go to the shops of smaller companies. She is afraid of fraud and therefore does not want to give away her credit card information.
Together with some colleagues Inga is working as a freelancer on different projects, some of them

are also involving photography and art design. They exchange their ideas and drafts on a collaborative workspace. Therefore every member of this community has access to the current version of the project.

## *Josha Fazekas*

19 years/ male/ Hungary

"I want to stay in contact with my friends – wherever they are."

| | |
|---|---|
| **Date of Birth** | 12th November 1989 |
| **Description** | Josha just started studying and moved 200 km to live next to the university. He is working part-time on various occasions to earn some additional money. Josha plays the guitar in a rock band and has some gigs on the weekend. |
| **Social Situation** | The girlfriend of Josha is currently abroad on an exchange program. Josha is living in a shared apartment with 2 friends. |
| **Health Situation** | Josha is wearing glasses, but he is of very good health. |
| **Financial Situation** | Since Josha just started studying he is dependent on his parents and the scholarship he gets. Nevertheless the money earned from occasional jobs allows him to buy additional things. |
| **Technological Knowledge and Usage of Technology** | Josha got his first mobile phone about 8 years ago. He likes to take pictures at parties with the integrated camera of his phone. Besides this he uses his phone to write messages and make calls. When he is bored or waiting for someone, Josha plays games on his mobile phone. Josha has his own laptop that he needs for his study work. He is familiar with office programs and runs the website of his band, which also includes a blog. He also uses his laptop to record demos from his band. |
| **Web- usage** | He surfs on the internet on a daily basis and uses it to stay in contact with his friends at home. Every day he spends about one hour talking (also using a webcam) to his girlfriend who is currently abroad. Furthermore he uses the internet to research for his studies and to find out about possible gigs for his band.<br>What he does online: |

- Social networking (just joined social networks before he started studying)
- Internet telephony
- E-Mails
- Website of his band
- E-shopping
- Online video sharing
- Music downloading/file sharing
- Selling his bands' music online
- Information retrieval

Josha has internet access at the university and shares a broadband connection with his flat mates.

**Negative Experiences**

Since Josha is very active on the internet he gets a lot of SPAM and unwanted internet telephony connection-requests.
Once he found out that somebody illegally published a track of the new album of his band.

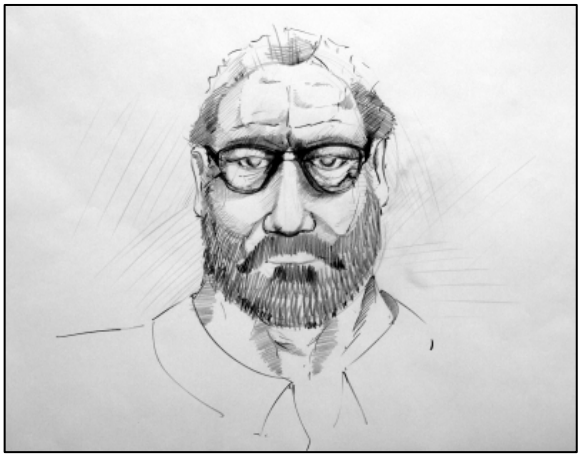
**Wish list**

He wants to actively master the type and amount of data published about him (e.g. e-mail address on social networking sites) to avoid SPAM e-mails. Also data given away to diverse organizations (e.g. clubs) should be kept private.
Since Josha tries to get serious jobs over social networks, it is important that his profiles are separated. He uses different aliases for different purposes – his boss should not find out about his private activities.

**Additional Information**

Josha's English is not the best and therefore he has problems understanding some of the privacy disclaimers (formulated too difficult).
He hasn't changed the default privacy settings of the social networks he is in and doesn't know much about privacy and data protection in general. Although he is concerned about privacy, his public profile includes birth date, the city he is living in, the name of his girlfriend and his interests.

## *Frank Falk*



76 years/ male/ United Kingdom

"I like to meet people who have the same interests as I do."

| | |
|---|---|
| **Date of Birth** | 18th April 1932 |
| **Description** | Since Frank retired about 15 years ago from his job as an electrician, he has been focusing on his hobbies. He likes to go fishing, but since he has no car he needs his son to go with him. |
| **Social Situation** | Frank was happily married to Margaret for over 40 years. 7 years ago Margaret passed away because of cancer. Frank has 2 children, a daughter (53) living abroad and a son (45) who lives around the corner. |
| **Health Situation** | About 5 years ago Frank started forgetting things and his eyes got bad. Now he has problems seeing, but also problems with his hips and arthritis have made it harder for him to walk. |
| **Financial Situation** | Frank earns a small pension that allows him to live an adequate life. |
| **Technological Knowledge and Usage of Technology** | Frank owns a mobile phone that he got as a present for his birthday 6 years ago. Since his wife died his children wanted to reach him at any time to check on him and not to make him feel lonely. Frank is able to call people with his mobile phone and receive calls, but not to use it further. Ten years ago he and his wife got a used computer from their son. Margaret, a retired secretary used it to store and safe recipes. Frank was not particularly interested in using the computer since it was too complicated to be used. Nevertheless 2 years ago he got a new computer from his son, who set it up in order to be easily used for reading news. Frank is still unsure about using the computer and he contacts his son as soon as something unexpected happens (e.g. pop-up menus, firewall). |

**Web- usage**

Frank has also got internet access (ISDN) and uses it about 3 times a week. According to him a slower connection (dial-in) would suffice as well.
What he does online:

- E-Mail (with his daughter – he needs time for typing though)
- Hobbies (Fishing websites)
- Medical information (doctors)
- Communities (Frank gets in contact with other people over the internet since it is hard for him to leave the house without help; he likes to read what other people post)

**Negative Experiences**

Frank is still uncertain when using the computer. He is not good at handling the mouse and okay at typing with 2 fingers. Since he has bad eyesight it happens that websites are hard to navigate and cumbersome.
Frank is overburdened when websites require information to be entered (e.g. login, online-shopping). Furthermore he does not like to enter data on websites because he does not fully trust the internet.
For him it is hard to distinguish which tool he should use for what (e.g. Outlook for e-mails and Internet Explorer for surfing). Frank does not understand the difference between his computer and the internet. Hence once he posted some private information on a website instead of writing it in a text-file.
Although his son configured a junk-filter for his e-mails, Frank still gets a lot of SPAM mail and ends up reading them for a while until he realises that it is SPAM.
He does not want to depend on the help of his son all the time.

**Wish list**

Frank wants the websites he uses to be very easy and understandable. Since he has bad eyesight, long dialogues tire him. He likes to enlarge the font size of the text.
Frank also wants to exactly know which information is needed and where it has to be entered – otherwise he needs the help of his son.

**Additional Information**

When Frank does not use the computer and/or the internet for some days, he has problems remembering how to use it. His son then has to explain everything once again. Furthermore Frank does not understand what privacy in this context means.

## *Hannes Obermaier*

35 years/ male/ Germany

"My family comes first, but I have hobbies too."

| | |
|---|---|
| **Date of Birth** | 3rd June 1973 |
| **Description** | Hannes Obermaier is an early adopter concerning new technologies. He works as a salesman in a big electronic company. Since he was a teenager Hannes always bought the latest technology. He still owns a Commodore C64. He likes playing computer games and therefore also has an XboX 360 and a PlayStation 3. Hannes has also a semi-professional home cinema in his living room. For his daughter he bought a wii, since the controls are easier to handle for her. |
| **Social Situation** | He is married to Sabine (33) for 3 years and has 2 children, Sebastian (6 months) and Michaela (2 years). |
| **Health Situation** | Hannes is a bit overweight. |
| **Financial Situation** | About 2 years ago Hannes and his wife bought a flat and they are still paying the interest. He spends a lot of his money for gadgets and latest technology. |
| **Technological Knowledge and Usage of Technology** | Hannes uses mobile phones since 1995 and before that he used car phones. He uses his mobile for making calls and playing games. Sometimes he also uses the browser of his phone. Hannes only writes few messages. Because of his affinity to technology, Hannes has owned many computer systems. Nevertheless he is still more user than developer, although he has some programming experience.<br>Since his children were born he has not enough time for programming experiments and therefore concentrates on playing computer games and online gambling. Recently he has taken a course in basic video editing to put videos of his children online. |

| | |
|---|---|
| **Web- usage** | Hannes is online almost every day, when his kids are in bed.<br>What he does online:<br>• Gaming<br>• Gambling<br>• Private web page (with pictures and ultrasounds of his newborn)<br>• Online video sharing (but more watching)<br>• Social networks (he stays in contact with his gaming buddies and colleagues)<br>Hannes just upgraded his broadband connection to a faster one. |
| **Negative Experiences** | For some gambling websites it takes ages to log in. Hannes always gets impatient when he has to click on a lot of buttons to get where he wants to go.<br>Once Hannes has accidentally sent private bank account information to a stranger instead of a friend. Since then he does not fully trust online transactions and started using privacy enhancing technologies. Nevertheless he got frustrated many times since he thinks that this technology is too complicated and the settings are too difficult. |
| **Wish list** | Hannes wants to efficiently combine his family live with his hobbies. For him it is important to just log in and play a game without a lot of problems and time consumed. He doesn't want his gambling statistics to be seen by anyone (e.g. opponents).<br>Hannes wants to decide which information his working colleagues are allowed to see.<br>Since his daughter started using the computer recently by clicking around, he wants to make sure that she does not send delicate information to the internet (e.g. private files, pictures, credit card number).<br>Hannes wants to undo possible privacy breaches. |
| **Additional Information** | Hannes' internet use is very dependent of his family life. When his kids are sick or he is on holidays, he might not be online for weeks. |

## *Mariangela Fiore*

15 years/ female/ Italy

"I like to talk to people about things that interest me."

| | |
|---|---|
| **Date of Birth** | 16th May 1993 |
| **Description** | Mariangela is a high school student that likes to stay in contact with her friends and wants to meet new people. |
| **Social Situation** | Mariangela is still living with her parents. Besides her friends at school she has some pen pals in different countries. |
| **Health Situation** | Mariangela is a healthy child. |
| **Financial Situation** | Her parents give Mariangela a monthly allowance of 60 €. With that money she has to pay for her mobile phone, food (outside her parents' house), clothes and other expenses. |
| **Technological Knowledge and Usage of Technology** | Since the age of 11 Mariangela has her own prepaid mobile phone. She talks to her friends and writes messages several hours a day. Mariangela's father is the manager of a small business and has taught her how to use the computer at an early age. She knows the major office programs, browsers and e-mail clients. One year ago Mariangela got a new MP3 player for her birthday. She likes to listen to her favourite pop groups while waiting for the bus. |
| **Web- usage** | During boring lessons in school Mariangela likes to play small flash-games. Furthermore she likes to chat in chat rooms during lessons or in the evenings at home. Nevertheless her time spent on the internet is strictly controlled by her mother, a housewife.<br>Mariangela also uses the internet to get information for her homework. She is very passionate about her dog and actively participates in a dog-forum. Furthermore Mariangela started a blog some time ago where she shares information about herself |

and pictures of her dog.
What she does online:

- Instant Messaging, Chats (she keeps in contact with her friends)
- Music downloads, picture sharing
- Social networks (she keeps in contact with friends and classmates, meet new people)
- E-Mail
- Information retrieval (school page, news, special interests)
- Forums (dog forum – she actively participates in discussions)
- Games (flash-based)
- Blog

Mariangela uses the internet at school and at home at her parent's place (broadband).

**Negative Experiences**

Sometimes strange people join her chat rooms and start writing naughty things.
Once a strange man called her on her mobile phone. He was trying to talk her into meeting him. He mentioned that he got her number from a pet forum. Mariangela hasn't looked into this forum for some time and was not aware that she disclosed this information. She then removed her number from all of her profiles.

**Wish list**

Mariangela wants to restrict the information seen about her to her friends only. Her parents should not be able to trace back everything she has done on the computer (especially when she was chatting about them).
She wants to be able to share her thoughts without any consequences.

**Additional Information**

Mariangela is influenced by peer pressure. As soon as her friends discover some new forums etc. she also joins them.
She is an average pupil, who is very much into animals. Besides horseback riding she is not doing any sports.

## *Eugene "black gene" Wade*

33 years/ male/ USA

"I can find every kind of information – just pay me."

| | |
|---|---|
| **Date of Birth** | 28th August 1975 |
| **Description** | Eugene is 33 years old and is currently working as a web designer at a big advertising agency. Besides his job he has a second income which is very lucrative. Eugene sells personal data for money on the internet. On the internet he uses his pseudonym "black gene". |
| **Social Situation** | Eugene is single. |
| **Health Situation** | Eugene is very healthy. Nevertheless he likes fast food very much. |
| **Financial Situation** | Since Eugene started his second job, he has enough money. He earns more money by selling private information than he earns for working in the advertising agency. |
| **Technological Knowledge and Usage of Technology** | Eugene is a computer geek. He has studied media design at a college and has learned some programming languages. Since Eugene likes almost everything that has to do with computers, he has learned some programming languages by himself. So far he knows C, C#, C++, Java, Ruby, PHP, JavaScript, Python, Perl, CGI and Ruby on Rails.<br>Eugene currently has 6 different computers with various operating systems at home (Unix, Linux, Windows, Mac OSX). He is very experienced in the field of computer hardware and has also knowledge in the field of cryptography. Eugene has acquired most of his knowledge by himself and these skills allow him to effectively harvest personal data. He also uses social skills that he accomplished through his work at the advertising agency for gathering data. |

| | |
|---|---|
| **Web- usage** | At home and at the advertising agency, Eugene has high-speed internet access. He uses the web daily for working and private purposes as well as to gather and sell personal data.<br>What he does online:<br>• Standard interaction (E-Mails, surfing, browsing, forums, chatting, etc.)<br>• Social engineering (by phone, social networks, etc.)<br>• Hacking/cracking of file servers, passwords, etc.<br>• Administration of a website<br>• Downloading, file sharing (software, music, movies, etc.)<br>Z is almost permanently online. |
| **Negative Experiences** | Once Eugene got caught by the government. They discovered him when he tried to crack a central database. Eugene got sent to prison for 2 weeks and had to pay 5.000 Euros compensation for the damage he caused. |
| **Wish list** | Eugene wants to cover his tracks so that the government cannot find him. Therefore he needs privacy of his data and actions. |
| **Additional Information** | Eugene delivers any kind of data/information for money. He uses different ways to gather his data. Eugene even calls people to get private information. His buyers are large companies working in different fields such as advertising or big companies competing against each other or looking for information about their employers.<br>He especially likes unsecured wireless networks. For Eugene this is the easiest way to gather personal information. Nevertheless he can crack all currently available systems.<br>Especially social networks Social networks make it easier for Eugene to gather information, since many people disclose private details to everybody.<br>Eugene is very interested in privacy enhancing technologies for two reasons: he can use them to stay private and he can use them (crack them) to get private information about other people. |

## *Ines Rüegg*

27 years/ female/ Switzerland

"I like talking to people."

| | |
|---|---|
| **Date of Birth** | 7th February 1981 |
| **Description** | Ines is 27 years old and works as an insurance representative at a rather large insurance company. She is permanently in contact with clients and therefore has good social skills. Ines likes to be in contact with people, but hates the "paperwork" on the computer. |
| **Social Situation** | Ines has a fiancée but they have not moved in yet. |
| **Health Situation** | Generally Ines is quite healthy and she does some sports on a regular basis. |
| **Financial Situation** | Ines has enough money to cover all her expenses (lower average). |
| **Technological Knowledge and Usage of Technology** | Ines knows the common Windows systems and office software. For her computers are mysterious tools that she does not really understand, but uses to get online.<br>Ines is very curious and likes to click on everything that moves across the screen. Ines generally clicks OK until she gets to the content of a website. She opens all E-Mails and likes to click away annoying alert messages from her firewall without reading them. Sometimes she unintentionally disables the firewall or the virus scan.<br>Ines' computer (a rather old machine) is regularly infected and turns into an ADSL-Zombie. She generally dislikes passwords and usually only uses one password to log into several systems or websites. If she has to change a password she usually writes it down on a sticky note to remember it. |

| | |
|---|---|
| | If her computer does not function right, Ines gets help from her boyfriend who has to regularly re-install her system because it breaks down. As compensation she helps him with his problems in tax administration. |
| **Web- usage** | She uses internet daily for work and private purposes. Ines has high-speed internet access because her boyfriend organized it for her.<br>What she does online:<br>• Member of social networks (more than 500 contacts)<br>• Browsing<br>• Shopping<br>• P2P music downloads of the latest charts (to be played on her ipod)<br>• E-Mails<br>• Forums |
| **Negative Experiences** | Ines catches almost every virus there is. Her hard drive gets destroyed frequently and she loses all her data.<br>Once private data (that was stolen from her computer) turned up on the internet.<br>Another time Ines' colleagues sent a prank e-mail from her account to the company mailing list since they knew where she keeps the sticky notes with her passwords. |
| **Wish list** | Ines wants the internet to be safe, without virus, trojans or worms.<br>She does not like to remember that many passwords. |
| **Additional Information** | Ines usually mixes up her private and professional space. She has very good communication skills and can be considered a people person.<br>Ines has lost a lot of data (especially personal pictures) due to viruses on her computer. |

## *Florence Hervieux*

42 years/ female/ France

"I want to be successful."

| | |
|---|---|
| **Date of Birth** | 6th October 1966 |
| **Description** | Florence is successfully working as an international manager since about 12 years. She is 42 years old and works for a French company since about 3 years in the position of a key account manager. After graduating from university 17 years ago she started working in the customer relations department of a software company. For carrier purposes Florence decided to finish a PhD in the area of business economics and immediately got a job in as a customer relations manager. |
| **Social Situation** | Florence is a single parent of a 6 year old boy (Daniele). She does not have much time, especially since Daniele needs a lot of attention. |
| **Health Situation** | Generally Florence is healthy, but stressed since she has to take care of her son and has a leading management position at the same time. |
| **Financial Situation** | Florence earns very well and does not care much about money. |
| **Technological Knowledge and Usage of Technology** | Florence knows the common Windows systems and office software as well as the company's proprietary software.<br>Florence is using mobile phones since about 15 years. Currently she has a company phone that she has always with her. She needs it to check her e-mails when she is out of her office. Furthermore she wants to be reachable in case Daniele needs something.<br>Florence also has a company laptop that she takes with her to the customers. If something does not work, Florence simply calls up the IT department. |

| | |
|---|---|
| **Web- usage** | Florence uses the internet on a daily basis, but mostly only for work-related purposes. She does have internet at home, but is only online when Daniele sleeps – otherwise she does not have time.<br><br>What she does online:<br>• Working<br>• Job search<br>• Browsing<br>• Shopping<br>• E-Mails |
| **Negative Experiences** | Florence was using social networks for her job applications. She found out that it was possible to google her information/profile. Therefore she deleted all her accounts. |
| **Wish list** | Florence is currently applying for a new job and only wants the right people to see her applications/job profile. Her current employer should not be able to find out about her wanting to change jobs.<br>She wants to hire babysitters over the internet and wants to know if she can trust the website/forum. |
| **Additional Information** | Florence is always stressed and does not have time to double-check everything she enters in a browser. Since she is working with customers, Florence has very good communication skills.<br>At work Florence deals with sensitive data on a regular basis. |

# 3 References


Cooper, A. 1999 The Inmates are Running the Asylum. Macmillan Publishing Co., Inc.

Gilbert, D. 2006. If only gay sex caused global warming. Los Angeles Times, July 2, 2006.

McGinn, J. and Kotamraju, N. Data-driven persona development, in: CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, Florence, Italy, pages 1521-1524, ACM, 2008

Nieters, J. E., Ivaturi, S., Ahmed, I., and Ahmed, I. 2007. Making personas memorable. In CHI '07 Extended Abstracts on Human Factors in Computing Systems (San Jose, CA, USA, April 28 - May 03, 2007). CHI '07. ACM, New York, NY, 1817-1824. DOI= http://doi.acm.org/10.1145/1240866.1240905

Pruitt, J. and Adlin, T. 2005 The Persona Lifecycle: Keeping People in Mind Throughout Product Design (The Morgan Kaufmann Series in Interactive Technologies). Morgan Kaufmann Publishers Inc.

Pruitt, J. and Grudin, J. 2003. Personas: practice and theory. In Proceedings of the 2003 Conference on Designing For User Experiences (San Francisco, California, June 06 - 07, 2003). DUX '03. ACM, New York, NY, 1-15. DOI= http://doi.acm.org/10.1145/997078.997089

Shyba, L. and Tam, J. Developing character personas and scenarios: vital steps in theatrical performance and HCI goal-directed design, in: C&C '05: Proceedings of the 5th conference on Creativity & cognition, London, United Kingdom, pages 187-194, ACM, 2005

# Bibliography


[ACC+05] Christer Andersson, Jan Camenisch, Stephen Crane, Simone Fischer-Hübner, Ronald Leenes, Siani Pearsson, John Sören Petterson, and Dieter Sommer. Trust in PRIME. In *Proceedings of the 5th IEEE Int. Symposium on Signal Processing and IT*, Athens, Greece, December 2005.

[AR97] P. E. Agre and M. Rotenberg. Technology and Privacy: The New Landscape. *Cambridge MA: MIT Press*, 1997.

[Ben98] Jan Panero Benway. Banner Blindness: The Irony of Attention Grabbing on the World Wide Web. *Proceedings of the Human Factors and Ergonomics Society 42nd Annual Meeting*, 1998. Rice University Research, Houston, Texas.

[Ber08] Mike Bergmann. Generic Predefined Privacy Preferences for Online Applications. In Simone Fischer Hübner, Penny Duquenoy, Albin Zuccato, and Leonardo Martucci, editors, *The Future of Identity in the Information Society: Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School*, International Summerschool Karlstad, Sweden, May 15 2008. Springer.

[Ber09] Mike Bergmann. Testing Privacy Awareness. *Lecture Notes in Computer Science; Proceedings of the IFIP/FIDIS Internet Security and Privacy Summer School, Masaryk University Brno, 1-7 September 2008*, to appear/2009.

[Bro96] J. Brooke. SUS: A Quick and Dirty Usability Scale. In *Usability Evaluation in Industry*, pages 189–194, London, United Kingdom, 1996. Taylor & Francis.

[BRP05] Mike Bergmann, Martin Rost, and John Sören Pettersson. Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology. In *Proceedings of the Fourteenth International Conference on Information Systems Development*, Karlstad, August 2005. Springer-Verlag.

[CKU08] CURE, KAU, and ULD. H 4.1.1 User Evaluation Plan. PrimeLife Heartbeat, June 2008.

[CL01] J. Camenisch and A. Lysyanskays. Efficient Non-Transferable Anonymous Multi-Show Credential System with Optional Anonymity Revocation. In

*Advances in cryptology, EUROCRYPT*, pages 93–118, New York, 2001. Springer.

[Cla07] Sebastian Clauß. *Towards Quantification of Privacy Within a Privacy–Enhancing Identity Management System*. PhD thesis, Technische Universität Dresden, Saxony, Germany, 2007.

[CMN80] Stuart K. Card, Thomas P. Moran, and Allen Newell. The Keystroke-Level Model for User Performance Time with Interactive Systems. *Commun. ACM*, 23(7):396–410, 1980.

[Coo99] Alan Cooper. *The Inmates are Running the Asylum*. Sams, Indianapolis, Indiana, 1. edition, 1999.

[Cou95] Council of Europe. Data Protection Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995. Official Journal L No. 281, 23.11.1995.

[DD08] Rachna Dhamija and Lisa Dusseault. The seven flaws of identity management: Usability and security challenges. *IEEE Security and Privacy*, 6(2):24–29, 2008.

[ECH08] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *CHI 2008 Proceedings*, pages 1065–1074, 2008. CHI 2008, April 5 - 10, 2008, Florence, Italy.

[FHPB+09] Simome Ficher-Hübner, John-Sören Pettersson, Mike Bergmann, Marit Hansen, Siani Pearson, and Marco Cassasa Mont. *The PRIME Book*, chapter HCI Designs for Privacy-enhancing Identity Management, pages 1–1000. Springer, 2009. Hopefully 2009 - just a placehoder.

[Gar05] Simson L. Garfinkel. *Design principles and patterns for computer systems that are simultaneously secure and usable*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2005. Adviser-Clark,, David D. and Adviser-Miller,, Robert C.

[GS05] Oliver Günther and Sarah Spiekermann. RFID and the Perception of Control: The Consumer's View. *Communications of the ACM*, 48(9):73–76, September 2005.

[Hor06] Kasper Hornbaek. Current Practice in Measuring Usability: Challenges to Usability Studies and Research. *International Journal of Human-Computer Studies*, 64(2):79–102, February 2006.

[HS07] Almut Herzog and Nahid Shahmehri. User help techniques for usable security. In *CHIMIT '07: Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, page 11, New York, NY, USA, 2007. ACM.

[IH07] Giovanni Iachello and Jason Hong. End-user privacy in human-computer interaction. *Foundation and Trends in Human-Computer Interaction*, 1:1–37, 2007.

[JEL03] J. Johnston, J. Eloff, and L. Labuschagne. Security and Human Computer Interfaces. *Computers & Security*, 22(8):675, 2003.

[Kru88] R.A. Krueger. *Focus groups: A Practical Guide for Applied Research*. Sage Publications, Newbury Park, CA, 1. edition, 1988.

[KW09] Christina Köffel and Peter Wolkerstorfer. PrimeLife Virtual Usability Laboratory – Results of Trial 1. *PrimeLife poject, internal report*, 2009.

[Lin08] Maria Lindström. Second Usability Tests on IPV3, January 2008. PRIME project, http://www.prime-project.eu.

[Lin09] Maria Lindström. Usability Test Report - Pilot Tests of Trust Evaluation (unpublished). Technical report, Karlstad University, 2009.

[MC04] George R. Milne and Mary J. Culnan. Strategies for Reducing Online Privacy Risks: Why Consumers Read [Or don't Read] Online Privacy Notices. In *Journal of Interactive Marketing*, volume 18, pages 15–29, 2004.

[NIA07] James E. Nieters, Subbarao Ivaturi, and Iftikhar Ahmed. Making Personas Memorable. In *CHI '07: CHI '07 extended abstracts on Human factors in computing systems*, pages 1817–1824, New York, NY, USA, 2007. ACM.

[Nie04] Jacob Nielsen. Jacob Nielsen's Alertbox, User Education Is Not the Answer to Security Problems, October 25, 2004. http://www.useit.com/alertbox/20041025.html, last accessed Nov 11, 2008.

[NM94] J. Nielsen and R.L. Mack, editors. *Usability Inspection Methods*. John Wiley & Sons, New York, NY, 1. edition, 1994.

[PA06] John Pruitt and Tamara Adlin. *The Persona Lifecycle: Keeping People in Mind Throughout Product Design*. Morgan Kaufmann, San Francisco, 1. edition, 2006.

[Pet08] John Sören Pettersson. (Ed.) HCI Guidelines, PRIME Deliverable D6.1.f. *PRIME Deliverable*, 2008. version 1 February 2008, https://www.prime-project.eu/prime_products/reports/arch/.

[PFHND+05] John Sören Petterson, Simone Fischer-Hübner, Jenny Nilsson Ninni Danielsson, Mike Bergmann, Thomas Kriegelstein, Sebastian Clauss, and Henry Krasemann. Making PRIME Usable. In *SOUPS*, Carnegie Mellon University, USA, July 2005. ACM Digital Library.

[PG03] John Pruitt and Jonathan Grudin. Personas: Practice and Theory. In *DUX '03: Proceedings of the 2003 Conference on Designing for User Experiences*, pages 1–15, New York, NY, USA, 2003. ACM.

[PH01] Andreas Pfitzmann and Marit Hansen. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In *Proceedings of WS on Design Issues in Anonymity and Unobservability*, Designing Privacy Enhancing Technologies, LNCS 2009, Proceedings of the Fourteenth International Conference on Information Systems Development, Heidelberg, August 2001. LNCS. Revised version 0.31 of Feb. 15st 2008; Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management–A Consolidated Proposal for Terminology.

[PKHvB03] A.S. Patrick, S. Kenny, C. Holmes, and M. van Breukelen. *Handbook for Privacy and Privacy-Enhancing Technologies*, chapter Chapter 12 - Human Computer Interaction, pages 249–290. Colege bescherming persoonsgegevens, 2003.

[SMP08] Dieter Sommer, Marco Casassa Mont, and Siani Pearson. PRIME Architecture V3. *PRIME project, public deliverable D14.2.d*, 2008.

[ST05] Lori Shyba and James Tam. Developing Character Personas and Scenarios: Vital Steps in Theatrical Performance and HCI Goal-Directed Design. In *C&C '05: Proceedings of the 5th conference on Creativity & cognition*, pages 187–194, New York, NY, USA, 2005. ACM.

[Ste08] Sandra Steinbrecher. Mehrseitige Sicherheit in Reputationssystemen - Anforderungsanalyse und Umsetzungsmöglichkeiten (Dissertation). Technical report, TU Dresden, 2008.

[TS04] Thomas S. Tullis and Jacqueline N. Stetson. A Comparison of Questionnaires for Assessing Website Usability. In *UPA Conference*, Minneapolis, Minnesota, 2004. Usability Professionals' Association.

[WMG06] M. Wu, Robert C. Miller, and Simon L. Garfinkel. Security Toolbars Actually Prevent Phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Press, Montreal*, pages 601–610, 2006.

[Yee02] Ka-Ping Yee. User interaction design for secure systems. In *ICICS '02: Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290, London, UK, 2002. Springer-Verlag.