Trust and Assurance Control – UI Prototypes

Editors:	Simone Fischer-Hübner (Karlstad University)
	Jenny Nilsson (Karlstad University)
Reviewers:	Arnold Roosendaal (Tilburg University)
	Sandra Steinbrecher (TU Dresden)
Identifier:	D4.2.1
Type:	Deliverable
Version	1.0 (Final)
Class:	Public
Date:	June 24, 2009

Abstract

This deliverable presents User Interface (UI) prototypes for a Trust Evaluation Function, which has the purpose of communicating reliable information about trustworthiness and assurance (that the stated privacy functionality is provided) of services sides to end users. For the design of this trust evaluation function, we have followed an interdisciplinary approach by investigating social factors for establishing reliable trust, technical and organizational means, as well as HCI (Human Computer Interaction) concepts for mediating evaluation results to the end users. Three iterations of mockups of trust evaluation function UIs that were produced and tested at Karlstad University's Ozlab are presented and discussed.

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

Members of the PrimeLife Consortium

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

Disclaimer: *The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright 2009 by Karlstad University.*

List of Contributors

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

Chapter	**Author(s)**
Executive Summary	Simone Fischer-Hübner (Karlstad University)
Chapter 1: Introduction	Simone Fischer-Hübner (Karlstad University)
Chapter 2: Trust Parameters	Simone Fischer-Hübner (Karlstad University)
Chapter 3: HCI Challenges	Simone Fischer-Hübner (Karlstad University)
Chapter 4: Design Principles and Mockups	Simone Fischer-Hübner (Karlstad University), Jenny Nilsson (Karlstad University)
Chapter 5: Scenarios and Test Results	Maria Lindström (Karlstad University), Jenny Nilsson (Karlstad University)
Chapter 6: Related UI Approaches	Simone Fischer-Hübner (Karlstad University)
Chapter 7: Conclusions and Outlook	Simone Fischer-Hübner (Karlstad University)
Appendix A: User Interfaces tested in three Usability Test Sessions	Simone Fischer-Hübner (Karlstad University), Maria Lindström (Karlstad University), Jenny Nilsson (Karlstad University), John Sören Pettersson (Karlstad University). Besides, other Activity 4 partners, in particular Peter Wolkerstorfer (CURE), Christina Köffel (CURE) and Erik Wästlund (Karlstad University), contributed with design improvement proposals, which we have addressed.

Executive Summary

Trust plays a major role in privacy-enhancing identity management, because users do not only need to trust their own platforms to manage their personal data accordingly but also need to trust communication partners and their remote set of platforms that receives personal data to process their data in a privacy-friendly manner and according to the (business) agreements.

Within the PrimeLife work package 4.2 on "Trust and Assurance HCI", we have elaborated the user interface designs of a trust evaluation function which allows end users to evaluate the trustworthiness of services sides. For this, reliable information about trustworthiness of the services side as well as information about the assurance that the privacy functionality promised by a services side is provided needs to be communicated to the end user.

For the design of the trust evaluation function, we have first studied social trust factors for establishing reliable trust, which have then motivated our choice of trust parameters for the trust evaluation function. The chosen trust parameters mainly refer to the institutional layers of the social trust factor model by Leenes et al. (2005) comprising information provided by trustworthy independent monitoring and enforcing institutions, including information about privacy and trust seals certified by data protection commissions or independent certifiers, the appearance of a site on blacklists maintained by consumer organisations, as well as information about the appearance security & privacy alert lists, such as anti-phishing alert lists. Another trust parameter that we have chosen measures the site's benevolence to implement privacy-enhancing PrimeLife functions. For this, dynamic seals can be used that can be generated in real-time by an "Assurance Evaluation component" at the services side.

For the design of user interfaces for a trust evaluation function, several HCI (Human Computer Interaction) challenges have to be met: The function has to illustrate parameters with different semantics and scopes (referring to both trustworthiness in terms of privacy and business reliability). Besides its has to address usability problems that we have observed from previous usability tests of prototypes developed by the PRIME project, namely the user's difficulty to differentiate between the user and the services side, as well as the phenomenon that extensive warnings can confuse the users that do not know how to react on them.

The following design principles have been applied for the UI (User Interface) design of our trust evaluation function comprising general HCI principles as well as specific design principles for addressing the challenges mentioned above:

- The use of a selection of meaningful overall evaluation results;
- The use of a multi-layered structure for displaying evaluation results on three levels (the overall result is shown on top level in situations where the user is requested to disclose data. The user can then click on a link leading to details of evaluation results of the individual trust parameters on the second level, which can be further expanded into a third level);
- The use of several UI concepts (text, colouring and icons in combination) for informing the users;
- Grouping of parameters into the categories "privacy" and "business reliability" to make clear that these are semantically different aspects of trustworthiness;
- Informing users without unnecessary warnings (i.e. the user is only warned about the more serious cases where a site appears on blacklists or alert lists, whereas in the case of

less serious results, such as that a site has no privacy seal, the user is only informed but no warning is displayed);

- Making clear that the services side (and not the user side) is evaluated by wording and structuring of the user interfaces.

Three iterations of mockups of trust evaluation function user interface prototypes were developed and tested with 10+10+12 test participants at Karlstad University's Ozlab. The usability tests clearly showed that our trust evaluation function is much appreciated by end users – almost all users would like to use a PrimeLife prototype including a trust evaluation function. Most test participants seemed to understand the presentation of overall evaluation results on top level as well as the fact that the services side was evaluated.

However, the tests also revealed some usability problems that we could not solve yet completed: In particular, some users had problems to understand the "neutral" evaluation result (in case that a site has no seal, is not supporting PrimeLife functions, is not blacklisted and does not appear on alert lists), which we first phrased with ”Not bad", "ok", and finally in the third mockup iteration with "fair". In the post-test interviews, there were no clear preferences for other names (such as "No alert"). The illustration of "neutral" results is one of the most difficult issues and still needs to be investigated further in our future work.

Contents

List of Figures

List of Tables

Chapter 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 her to trust the system*" (Johnston et al. 2004).

Usability tests of privacy-enhancing identity management prototypes performed within the EU FP6 project PRIME[1] have shown that there are problems to make people trust the claims about the privacy-enhancing features of the systems (see Fischer-Hübner and Pettersson 2004, Andersson et al. 2005). Although test users were first introduced into the aims and scope of privacy-enhancing identity management, the tests revealed that many of the test users did not trust the claim that the tested system would really protect their data and their privacy. Some participants voiced doubts over the whole idea of attempting to stay private on the Net. "Internet is insecure anyway" because people must get information even if it is not traceable by the identity management application, explained one test participant in a post-test interview. Another test subject stated: "It did not agree with my mental picture that I could buy a book anonymously". Another factor contributing to the lack of trust that was revealed by our usability tests was that test subjects generally had difficulties to mentally differentiate between user side and services side identity management. In post-test interviews the test subjects sometimes referred to functionalities from both the website and the user side identity management system as if these were one. Consequently, they also had difficulties to understand that the user side identity management console, where the user can manage her electronic identities, can be trusted by the user because it is within the user's control, whereas the website is under the service provider's control. Similar findings of a lack of trust in privacy-enhancing technologies were also reported by others, e.g. by Günther and Spiekermann in a study on the perception of user control with privacy-enhancing identity management solutions for RFID environments, even though the test users considered the PETs in this study fairly easy to use (Günther and Spiekermann 2005).

Trust plays a major role in privacy-enhancing identity management, because users do not only need to trust their own platforms to manage their data accordingly but also need to trust services sides and their remote set of platforms that receive personal data to process their data in a privacy-friendly manner according to their business agreements with the users.

[1] https://www.prime-project.eu/

For helping users to evaluate the trustworthiness of services sides, the focus has to be on mediating factors to the users that measure the vendor's actual trustworthiness and that support trustworthy behavior of a site (Riegelsberger et al. 2005).

The HCI (Human Computer Interaction) research in PrimeLife approaches this problem in order to enhance the users' trust in PrimeLife and its backend systems, by developing a trust evaluation function that can communicate reliable information about trustworthiness and assurance (that the stated privacy functionality is provided) of services sides during the process of trust and policy negotiation. For the design of this trust evaluation function, we have followed an interdisciplinary approach by investigating social factors for establishing reliable trust, technical and organizational means, as well as HCI concepts for mediating evaluation results to the end users.

The remainder of the document is structured as follows: In Chapter 2 (Trust Evaluation Parameters), we will discuss social trust factors, and how they have motivated the choice of trust parameters that we have chosen for the evaluation function. The underlying technical and organisational means for our trust parameters are mentioned and it is shown how information about those trust parameters are requested during the process of trust and privacy policy negotiation. In chapter 3, we briefly discuss HCI Challenges that need to be met when designing the user interfaces of a trust evaluation function and Chapter 4 is then presenting HCI Design Principles taking those challenges into account that we followed. In chapter 5, we are then presenting our trust evaluation function mockups. Chapter 6 is presenting the iterations of usability tests that we performed at Karlstad University and their results. In Chapter 7, we are briefly presenting related HCI approaches. Chapter 8 is finally providing conclusions and an outlook. Appendix A is presenting the complete set of user interface prototypes (mockups) that we have produced and tested in three iteration cycles.

This report is an updated and extended version of chapter 4 (HCI for Trust and Assurance Evaluation) of the HCI Research Report V1 (PrimeLife Deliverable D4.1.1). For the HCI research report, we had only reported our first research results based on our initial mockups and first iteration of usability tests, whereas this report presents our advanced results after three iterations, in which our mockups have been successively improved and tested.

Chapter 2

Trust Evaluation Parameters

For designing a trust evaluation function, an interdisciplinary approach has to be taken by investigating the social factors for establishing reliable trust[2], technical and organisational means, as well as HCI concepts for mediating evaluation results to the end users. In this chapter, we first elaborate social trust factors for establishing reliable trust (section 2.1). Then, we show how social trust factors have motivated our choice of trust parameters for the evaluation function and mention the underlying technical and organisational means (static seals, dynamic assurance seals, black and alert lists) for our chosen trust parameters (section 2.2). Finally, it is shown how information about those trust parameters are requested during the process of trust and privacy policy negotiation (section 2.3).

2.1 Social trust factors

A trust evaluation function has to be based on suitable parameters corresponding to social trust factors for measuring the actual trustworthiness of a communication partner in terms of privacy practices and of the reliability as a business partner and for establishing reliable trust. Social trust factors in the context of e-Commerce have already been researched by others.

For instance, Turner (2001) showed that for ordinary users to feel secure when transacting with a website the following factors play a role: 1. the company's reputation, 2. their experiences with the website, and 3. recommendations from independent third parties.

Riegelsberger et.al. (2005) present a trust framework which is based on contextual properties (based on temporal, social and institutional embeddedness) and the services side's intrinsic properties (ability, motivation based on internalized norms, such as privacy policies, and benevolence) that form the basis of trustworthy behavior. Temporal embeddedness can be signalled by visible investment in the business and the site, as e.g. visualised by professional website design, which can also be seen as a symptom for the vendor's intrinsic property of competence or ability to fulfil a contract. Taking the phenomenon into consideration that many users have problems to differentiate between user and services side, these factors of professional

[2] A good discussion of the terms trust and trustworthiness are available at the Stanford Encyclopedia of Philosophy, first published 20 February 2006, http://plato.stanford.edu/entries/trust/.

design should in general be taken into account for the UI (user interface) design of a PrimeLife trust evaluation function even though the trust evaluation function is not part of the vendor's website but part of the user side identity management system. Social embeddedness, i.e. the exchange of information about a services side's performance among users, can be addressed by reputation systems. Institutional embeddedness refers to the assurance of trustworthiness by institutions, as done with trust seal programs.

A model of social trust factors, which was developed by social science researchers in the PRIME project (Leenes et al. 2005), (Andersson et al. 2005), has identified 5 layers on which trust plays a role in online services: socio-cultural, institutional, service area, application, and media. Service area- related trust aspects which concern the trust put in a particular branch or sector of economic activity, as well as socio-cultural trust aspects can however not be directly influenced by system designers. Also control over the media layer-related trust aspects (i.e. trust in the Internet as a reliable medium) is limited for identity management system designers. More suitable factors for establishing reliable trust can be achieved on the institutional and application layers of the model, which also refer to trust properties (contextual property based on institutional embeddedness as well as certain intrinsic properties of a web application) of the framework by Riegelsberger et al. (2005). As discussed by Leenes et al. (2005), on the institutional layer, trust in a service provider can be established by monitoring and enforcing institutions, such as data protection commissioners, consumer organisations and certification bodies. Besides, on the application layer, trust in an application can be enhanced if procedures are clear, transparent and reversible, so that users feel in control. This also corresponds to the findings of Trustguide (2006), which provides guidelines on how cybertrust can be enhanced.

2.2 Chosen parameters and their underlying technical and organisational concepts

Taking results of these studies on social trust factors into consideration, we have chosen the following parameters for evaluating the trustworthiness of communication partners that mainly refer to the institutional and application layers of the social trust factor model.

Information provided by trustworthy independent monitoring and enforcing institutions, which we are utilising for our trust evaluation function, comprise:

- Privacy and trust seals certified by data protection commissioners or independent certifiers (e.g., the EuroPrise seal[3], the TRUSTe seal[4] or the ULD Gütesiegel[5]).
- Blacklists maintained by consumer organisations (such blacklist exists for example in Sweden listing companies not following the National Board for Consumer Complaints' recommendations on how to settle consumer disputes)
- Security & privacy alert lists (such as alert lists for phishing sites, such as Google's anti-phishing blacklist. In future, privacy alert lists could also be maintained by data protection commissioners).

The European Consumer Centres have launched a web-based solution, Howard the owl, for checking trust marks and other signs of trustworthiness that could be used as well when evaluating a web shop[6].

[3] https://www.european-privacy-seal.eu/

[4] http://www.truste.org/

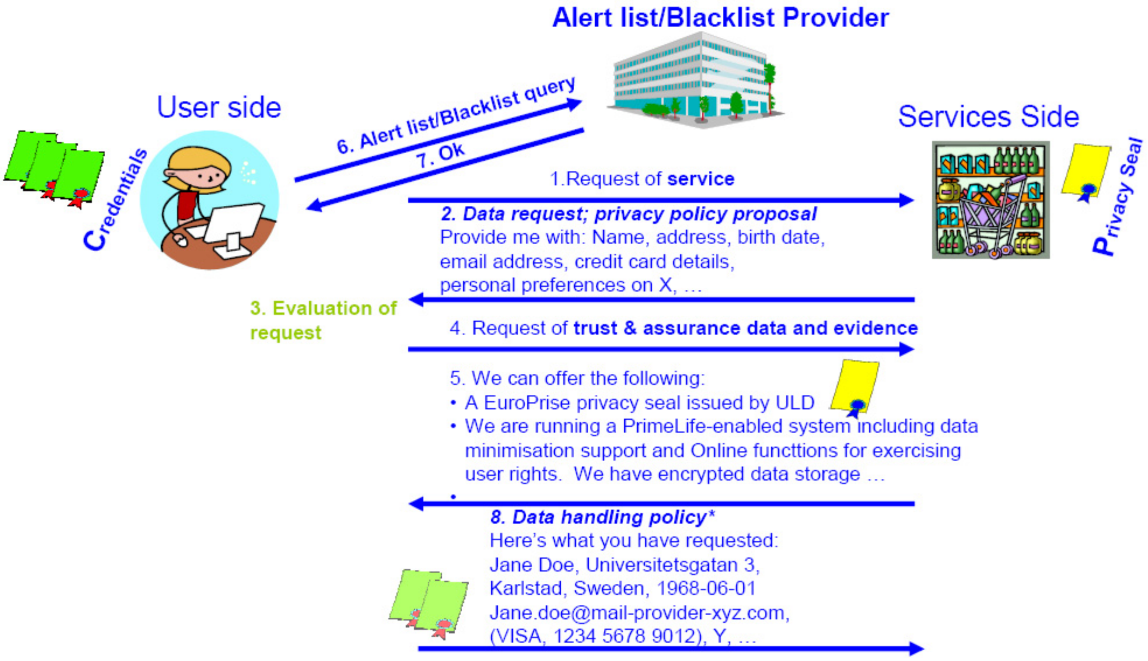
[5] https://www.datenschutzzentrum.de/guetesiegel/index.htm

[6] ready21.dev.visionteam.dk

Static seals can be complemented by dynamic (in real-time generated) seals conveying assurance information about the current security state of the services side's system and its implemented privacy and security functions. Such dynamic seals can be generated in real-time by an "Assurance Evaluation" component that has been implemented within the PRIME framework (Pearson 2006). 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 modeled as a third party that is not under full control of the services side. Such dynamic assurance seals can measure the intrinsic property of a services side's benevolence to implement privacy-enhancing functionality. Such functionality can comprise also transparency-enhancing tools that allow users to access, and to request to rectify or delete their personal data online (as implemented within the PrimeLife's work packages 4.2 in cooperation with 2.2), which will allow users to feel in control. As discussed above, this is important prerequisite for establishing trust. For our trust evaluation function, we therefore used dynamic assurance seals informing about the PrimeLife privacy-enhancing functions that the services side's system has implemented.

Also reputation metrics based on other users' ratings can influence user trust, as discussed above. Reputation systems, such as for instance the one in eBay, 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 whom it might for instance be difficult to judge the privacy-friendliness of communication partners. So far, we have therefore not considered reputation metrics for the PrimeLife trust evaluation function, even though we plan to address them in future research and versions of trust evaluations within the PrimeLife project.

2.3 Request and evaluation of trust parameters during the process of privacy and trust policy negotiation



2. Data request; privacy policy proposal
Provide me with: Name, address, birth date, email address, credit card details, personal preferences on X, …

4. Request of **trust & assurance data and evidence**

5. We can offer the following:
- A EuroPrise privacy seal issued by ULD
- We are running a PrimeLife-enabled system including data minimisation support and Online functtions for exercising user rights. We have encrypted data storage …
-

8. Data handling policy*
Here's what you have requested:
Jane Doe, Universitetsgatan 3,
Karlstad, Sweden, 1968-06-01
Jane.doe@mail-provider-xyz.com,
(VISA, 1234 5678 9012), Y, …

Figure 1: Privacy and trust policy negotiation in PRIME and PrimeLife

Following the process of trust and policy negotiation of the PRIME technical architectures (on which also PrimeLife systems are based), privacy seals, which are digitally signed by the issuing institution, as well as dynamic assurance seals can be requested from a services side directly (see steps 4-5 in Figure 1), whereas information about blacklisting and alerts need to be retrieved from the third party list providers (see steps 6-7 in Figure 1). When the user requests a service (step 1), the services side replies with a request of personal data and a proposal of a privacy policy (step 2). After evaluating the request and privacy policy (step 3), the user may want to evaluate the site's trustworthiness first, before making any decision. The user can then in turn request trust and assurance data and evidences from the services side, such as privacy seals and dynamic assurance seals (steps 4-5), and information about blacklisting or alerts concerning this site from alert list or blacklist providers (steps 6-7). Information about the requested trust parameters are then evaluated at the user side and displayed via the trust evaluation user interfaces along with the privacy policy information of the services side within the "Send Personal Data?" dialogue window (see Figure 3 below), with which also the user's informed consent for releasing the requested data for the stated policy is solicited. The user can then based on the trust evaluation results and policy information decide on releasing the requested personal data items and possibly adopt the proposed policy, which is then replied to the service provider (step 8).

Chapter 3

HCI Challenges

Designing the UI for a Trust Evaluation Function poses several challenges that need to be addressed. In particular, besides the challenge of finding appropriate trust parameters addressed in chapter 2, those trust parameters as part of the trust metrics that we are using also 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:

3.1 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, the parameters can have different semantics.

The user's trust in a services side will depend both on the services side's privacy and business practices – i.e. different aspects have to be measured. Parameters "Privacy seals", "Supports PrimeLife functions", "Mentioned in security and privacy alert lists" that we have chosen for our mockups (see below) measure the trust that users can put into that their data are processed in a secure, 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 services side is not listed on blacklists or on a security & privacy alert list are at least positive indications for the trustworthiness of a services side, whereas the result that a services 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 the future.

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

3.2 Find intuitive icons

Trust measures should also be illustrated by suitable 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.

3.3 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:

3.3.1 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 (see test reports for PRIME IPv3 reported in PrimeLife Deliverable D4.1.1).

3.3.2 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 services 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.

Chapter 4

Design Principles and Mockups

For the design of our trust evaluation function mockups, we followed the design principles listed below comprising general HCI principles as well as design principles, which should in particular address challenges and usability problems that we have encountered in previous usability tests (see chapter 3).

4.1 Use a selection of meaningful overall evaluation results

For simplification, the evaluation results are summarised into three possible overall results: “good”, “fair”, 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[7] – 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 also for informing them about positive trust indicators.

The naming of the third result, currently “fair”, has proven difficult. Several different names and smileys have been tested in the *three usability test* of our mockups conducted:

- “Not bad”, the grey colour and a neutral looking emoticon (😐) was used in the first test session, but this was confusing for the test participant and several interpreted it as meaning “not evaluated”.
- In the second test session “OK” and another neutral looking emoticon (😐), was used. This result was still interpreted as “not evaluated” by some participants while others interpreted the result as neutral or even trusted. In the pre-test interview “Not bad”, “No alarm” and “OK”, all with the same neutral smiley, were presented. When the participants were asked to chose the most popular alternative was “No Alarm”, preferred by four participants, followed by ”OK”, preferred by three participants, and ”Not bad”, preferred by two participants, (one participant did not like any of the alternatives).
- “Fair” in combination with a middle result on the trust meter (see Figure 2a) was used in the mockup during the third test session. As in the previous tests, this result was interpreted as

[7] http://www.mywot.com

"not evaluated" by some participants (four out of the twelve participants). When the participants later were asked to choose between "Fair" and "OK", in combination with a middle result on the trust meter, "Fair" proved to be the most popular alternative.

In order to make the middle result less confusing and to put it into context on a scale ranging from "poor" to "good", the idea of illustration the trust test result with emoticons was elaborated and a trust meter created, see Figure 2.

The emoticons used in the first two tests, Poor ☹ Good ☺ as well as the "Not bad/OK" emoticon described above, was in the third usability test replaced with the trust meter. The trust meter received some positive comments from the test participants. However, as previously mentioned, some participants still believed that the middle result represented a non-evaluation (i.e. the website had not been evaluated).

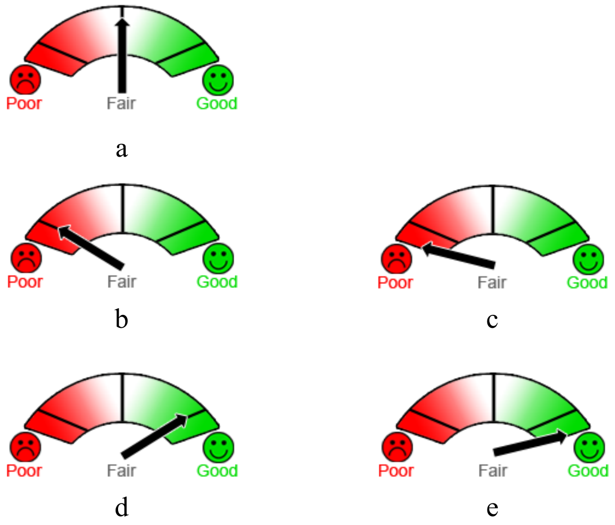


Figure 2: Trust Meter illustrating three different trust evaluation results

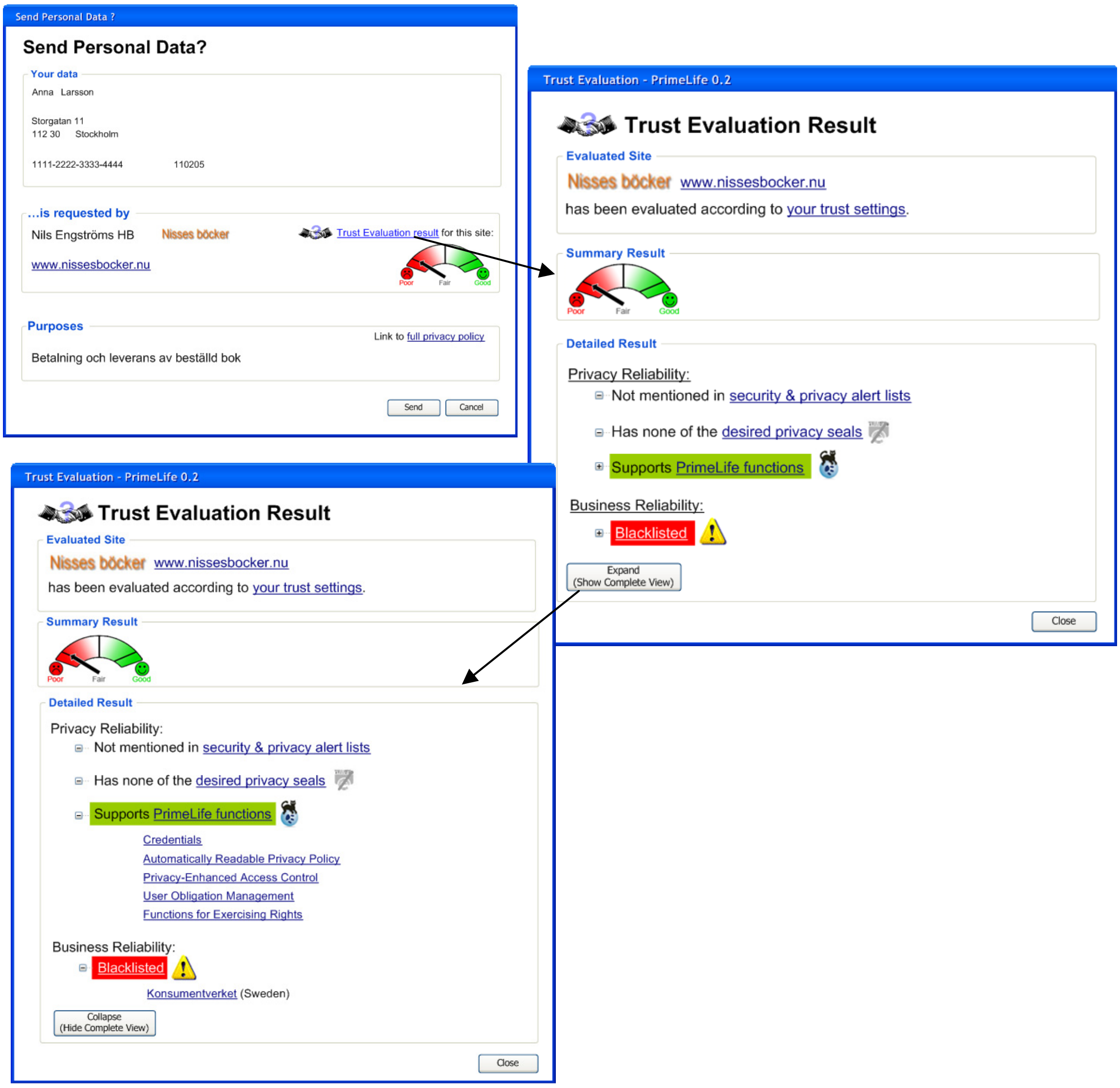
The following algorithm is used for calculating the overall results that are displayed on the top layer:

- A services side is rated as "fair" (illustrated by the meter shown in Figure 2a), if no positive (the services side has no privacy seals, no support of PrimeLife functions) and no negative (the services side does not appear on security & privacy alert lists or blacklists) evaluation results are reported.
- A services side is rated as "poor" (illustrated by the meter shown in Figure 2b) if it is either blacklisted or mentioned in security & privacy alert lists. If the services side is both blacklisted and appears on alert lists, the arrow of the trust meter points to the very left end of the meter (see Figure 2c).
- A services side is rated as "good" (illustrated by the meter shown in Figure 2d), if nothing bad can be reported (i.e., the services side is neither blacklisted nor appearing on security & privacy alert lists) and something positive can be reported (meaning that the services side has been awarded a privacy seal or supports PrimeLife functions). If the services side is neither blacklisted nor does it appear on alert lists, and if it has a privacy seals and supports PrimeLife functions, the arrow of the trust meter points to the very right end of the meter (see Figure 2e).

4.2 Use a multi-layered structure for displaying evaluation results

In our mockups, 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.

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 coloured emoticons accompanied by a short textual description and a meter indicating the overall trust evaluation result (see below and Figure 3). 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 security & privacy alert lists, black-listing, awarded privacy seals and 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 (see Figure 3).



Send Personal Data ?

Send Personal Data?

Your data

Anna Larsson

Storgatan 11
112 30 Stockholm

1111-2222-3333-4444 110205

...is requested by

Nils Engströms HB Nisses böcker

www.nissesbocker.nu

Trust Evaluation result for this site:

Purposes

Link to full privacy policy

Betalning och leverans av beställd bok

Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Site

Nisses böcker www.nissesbocker.nu

has been evaluated according to your trust settings.

Summary Result

Detailed Result

Privacy Reliability:

⊟ Not mentioned in security & privacy alert lists

⊟ Has none of the desired privacy seals

⊞ Supports PrimeLife functions

Business Reliability:

⊞ Blacklisted

Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Site

Nisses böcker www.nissesbocker.nu

has been evaluated according to your trust settings.

Summary Result

Detailed Result

Privacy Reliability:

⊟ Not mentioned in security & privacy alert lists

⊟ Has none of the desired privacy seals

⊟ Supports PrimeLife functions

Credentials
Automatically Readable Privacy Policy
Privacy-Enhanced Access Control
User Obligation Management
Functions for Exercising Rights

Business Reliability:

⊟ Blacklisted

Konsumentverket (Sweden)

Figure 3: Mockups providing multi-layered trust evaluation presentation

4.3 Make clear what is evaluated

The user interface should make very clear that the services side and not the client side is evaluated. For showing this, our mockups are clearly speaking about the trust evaluation results “for this site” on the top level after naming this site (see Figure 3, “Send Personal Data?”). 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 3, the “Send Personal Data?” window is also structured in three areas referring to the *data* requested, the services side that 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.

4.4 Use several UI concepts for informing users

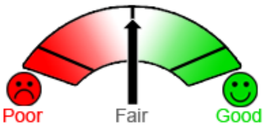
In our mockups, we use the different UI concepts of text, colouring and icons in combination, in order to inform the user about the evaluation results in an easily and intuitively understandable way. The text states the evaluation results unambiguously, while the colours “red” and “green” in addition mark “poor” and “good” overall and individual evaluation results. The result “fair” is not marked with a colour. The choice of colour, or lack thereof, for the “fair” result is described in Section 4.5.

The additional icons should enable users to quickly grasp these evaluation results. The following icons were chosen:

4.4.1 On top layer

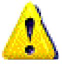
- For the trust evaluation function:

- For the overall evaluation results: (see Section 4.1 above):



4.4.2 On second and third layer

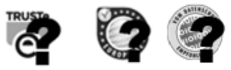
- For alarming the user:



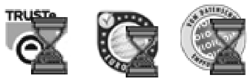
- For the evaluation result that a services side has a privacy seal (TRUSTe seal, EuroPrise seal, ULD Gütesiegel):

TRUSTe
EUROPRISE
VOM DATENSCHUTZ EMPFOHLEN

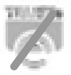
- For the evaluation result that a services side has not a specific seal or that there is at least no information about awarded seals:



- For the evaluation result that a seal once awarded for a services side has expired. These icons were used in test 1 (grey seal with an hour glass where the sand has already been running through):



- Since the icons with the question mark or hour glass above were not understood by the test participants they were replaced with another set of icon in test 2 and 3 (greyed out seals with a grey line crossing each of them). However, some participants still had difficulty determining what the icon represented:

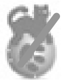


.

- 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). This icon was used in test 1:

- Since the icon with the black cat as depicted above was perceived as not "trustworthy" in test 1 it was replaced with another icon in test 2 and 3. This icon did not get any negative comments from the test participants:



4.5 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 services sides are blacklisted or appeared on security & 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 security & 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, the lack of colour is used to symbolise that no positive and no negative evaluation results are reported.

For previous PRIME mockups 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 first chose a more neutral grey for those cases. This was used in the first usability tests of our mockups conducted. The results of the test showed that several test participants believed that the website had not been evaluated, or that the grey colour indicated that the user had not made any settings for the marked parameter. In the second and third test session the grey colour was removed from the result presentation, since it could indicate a “not available”-state, and the naming was changed from “Not bad” to ”OK” in the second test and “Fair” in the third test, as described in Section 4.1.

4.6 Group parameters into categories

In the second and third iterations of mockups, we structured 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 alert lists, privacy seals and PrimeLife function support). This structure should illustrate that the trust parameter used have different semantics 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.

Chapter 5

Scenarios and Test Results

A total of three usability tests have been conducted with our three iterations of mockups during 2009; the first in January with ten test persons, the second in February, also with ten test persons, and the third in March-May, with twelve test persons. All test participants were Swedish.

The tests were performed in the Ozlab testing environment of Karlstad University. During the tests, the test leader was seated next to the test persons and made notes about the test persons' reactions. Screen actions were recorded and later analysed, and post test interviews were performed (Lindström 2009a, Lindström 2009b, Lindström and Nilsson 2009).

5.1 The scenarios and test users actions

The scenarios used in our three test sessions are presented in a summarised form in Table 1 below. In the table, the number of the tasks and the tasks themselves are described in italic, followed by the overall trust evaluation result in bold with the detailed trust parameters listed underneath. The scenarios have been divided into five different groups according to the trust evaluation result and detailed parameters in order to compare the three test sessions.

Scenario group #	Test 1	Test 2	Test 3
A	*1) Enter personal data into the PrimeLife system*	*1) Enter personal data into the PrimeLife system*	*1) Enter personal data into the PrimeLife system*
B	*3) Register as a customer at an unknown website);* **“Poor”** - Mentioned in privacy alert list (The Swedish Data Inspection Board) - Supports PrimeLife-functions *4) Register as a member at an unknown Slovenian website (bookshop);* **“Poor”** - Blacklisted (Austria) - Privacy seal (TRUSTe Seal) - Does not support PrimeLife-functions	*2) Register as a customer at an unknown website;* **“Poor”** - Blacklisted (Austria) - Supports PrimeLife-functions	*2) Register as a customer at an unknown website;* **“Poor”** - Blacklisted (Sweden) - Supports PrimeLife-functions *5) Register as a customer at an unknown online-ring tones website;* **“Poor”** - Supports PrimeLife functions - Blacklisted (Denmark)
C	*5) Register as a member at an unknown news website;* **“Not bad”** - Not mentioned on selected privacy alert lists - No privacy seals - Not blacklisted - Does not support PrimeLife-functions.	*3) Register as a member at an unknown online-game website;* **“OK”** - Not mentioned on selected privacy alert lists - No privacy seals - Not blacklisted - Does not support PrimeLife-functions	*3) Register as a member at an unknown online-game website;* **“Fair”** - Not mentioned on selected privacy alert lists - No privacy seals - Not blacklisted - Does not support PrimeLife-functions
D	*2) Register as a customer at a known Swedish website;* **“Good”** - Privacy seal (TRUSTe Seal) - Supports PrimeLife-functions		*4) Register as a member at an unknown online-movie website;* **“Good”** - Privacy seal (TRUSTe Seal) - Supports PrimeLife functions
E	*6) Register as a member at an unknown online-game website;* **“Good”** - Not mentioned on selected privacy alert lists - No privacy seals - Not blacklisted - Supports PrimeLife-functions		

Table 1: Scenarios used in the three trust test sessions

5.1.1 Scenario group A – enter personal data

All three usability test sessions started with the same scenario: the user was asked to enter personal data into the PrimeLife system since it was the first time the user used the system. All participants entered personal data without any problem. It was obvious that all of them had done similar actions before.

5.1.2 Scenario group B – "Poor"

In scenario group B the trust evaluation result was "poor" but the detailed parameters differed between the three usability tests. In the first and second test sessions all participants chose not to send personal data to the website. In the third test the result was the same with exception to one test participant; in scenario 2 he did not trust the evaluation and chose to send his personal information, the same choice was made in scenario 5 were he commented that the website was blacklisted in Denmark and he did not care about Danish blacklists. In the first test session two participants commented in scenario 4 that they thought it was strange that the site was blacklisted but still had privacy seal(s) and another three participants commented that the site did not support/was not controlled by/connected to the PrimeLife system. *"...this does not feel good since I have bought the PrimeLife system to protect me...".*

5.1.3 Scenario group C – "Not bad/OK/Fair"

The impression that the test leader got was that the trust evaluation result in group C was the most difficult for the participants to understand. Many different responses were made of what the result meant. Some persons interpreted the results as neither good nor bad but one participant in the first test also commented that *"According to the detailed result there is no result at all. Thus ′Not bad′ can mean ′not evaluated′.".* Two other participants came to the same conclusion, i.e. that the website was not evaluated. One person in the second test questioned how it is possible for the system to know if the website is okay or not if it does not support PrimeLife-functions. The confusion was also noticeable in the third test session, even though we used tool tips to better explain what a Support of PrimeLife functions should mean. Four participants believed that the website had not been evaluated, and one participant said: *"The website has behaved but they don't use the PrimeLife system, thus PrimeLife can not help me at all...".*

5.1.4 Scenario group D – "Good"

Since this was the second scenario in the first test session, it almost immediately became clear that the users had no problem understanding the green colour but the grey colour was confusing to some participants. In the third test session most participants finished the fourth scenario very fast and agreed to send data. Only one participant cancelled and commented that he had too vague information about PrimeLife to decide if they were trustworthy enough: *"The website has good recommendations but can I trust PrimeLife?".*

5.1.5 Scenario group E – "Good"

This scenario group was only presented in the first test session. Several participants commented that the smiley on the result summary was green and that they trusted that even though they did not fully understand the detailed results. One participant thought that *"If PrimeLife had checked this website it would have been green indications on the other results too.".*

5.2 Detailed test results

Answers to the questions posed in test 1

1) Is the workflow good?

Eight participants answered that the prototype was easy to navigate, the other two answered “to some extent”, they later elaborated when asked what was difficult: one of them answered “the cat” and the other the expand/collapse icons.

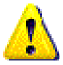
2) What is suitable name for the function(s) in question in English?

Seven out of ten participants wanted to call the control/evaluation the system performed “Trust Evaluation”, however, this was the expression used in the prototype. The other three suggested “Are they trustworthy?”, “Trust this partner” or something with the words “Trust” and “Check”.

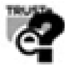
3) When do users want to have information on the individual evaluations: already in “Send Personal Data?” or by clicking on a summary of the evaluation result?

When asked when they want information on the individual evaluations seven participants answered that they wanted more information on the first layer, i.e. in the “Send Personal Data?” window. The remaining three wanted the same solution as seen in the prototype, i.e. by clicking on a summary of the evaluation result.

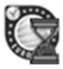
4) How do icons work at top-level (i.e. in the “Send Personal Data?” window) to indicate evaluation results?



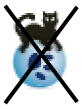
The icon for “Warning” was correctly understood by all participants.



This icon was interpreted as no information, not evaluated or not fulfilled.



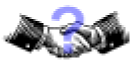
The hourglass was the most noticed part of this icon, the participants talked about time and waiting but none of them understood the icon.



Four participants gave a correct explanation of the icon, the remaining six had no guesses.

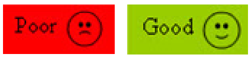
5) Should there be an icon for the evaluation function, and what should it look like?

Seven of the ten participants answered yes when asked, but they had very few ideas about how it should look. The two suggestions made were a star or the same icon as used but combined with text.

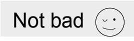


The icon used in the prototype was explained in several different ways by the participants in the pre-test interview, and four participants commented that they did not notice it during the test. Two test participants described it correctly.

6) How are the colours perceived on the second level?


Poor ☹ Good ☺

The colours red and green in the prototype (both on icons and over text) were all understood correctly by the participants.


Not bad ☺

The grey colour (both on icons and text fields) were confusing. The participants gave different explanations of how they perceived it; there were speculation that the site was not controlled, had done nothing wrong or information was missing. None of the participants gave an entirely correct description of the trust evaluation result for "Not bad".

7) Do people like this function?

Yes, all participants would like to use a product that controls the visited website.

Other findings

When asked which side the evaluation regarded (user's computer or the visited website) nine out of ten participants answered correct, the last participant thought that both services sides where evaluated.

<u>Answers to the questions posed in test 2</u>

1) Would a trust evaluation function make the PrimeLife system more trustworthy?

Yes, all participants thought that inserting the Trust Evaluation function will make the PrimeLife system more trustworthy.

2) Do users succeed to make a distinction between user and service side?

Yes, nine out of ten participants answered correct.

3) What is suitable name for the function(s) in question?

Eight out of ten participants wanted to call the control/evaluation the system performed "Trust Evaluation", however, this was the expression used in the prototype.

4) Are there any differences in how users perceive blacklisting from different countries?

The participants were asked to list how serious it is to be on a blacklist from Sweden, Austria and Slovenia:

- Swedish most serious and Slovenian least serious: 6 participants.
- Equally serious regardless country: 2 participants.
- Swedish and Austrian most serious: 1 participant.
- Austrian and Slovenian most serious: 1 participant.

The participants were asked to list how serious it is to be on an alert list from Sweden, Austria and Slovenia:

- Swedish most serious and Slovenian least serious: 4 participants.
- Equally serious: 3 participants.
- Slovenian and Austrian most serious: 2 participants.
- Slovenian most serious, Swedish and Austrian equally serious: 1 participant.

When asked to compare the seriousness of a Swedish blacklist with a Swedish alert list six participants thought it was most serious to be on a "Blacklist", three participants thought it was equally serious to be on a "Blacklist" and an "Alert list", and one participants thought it was most serious to be on an "Alert list".

5) Evaluate some alternative options for some of the icons

Three versions of the middle result were presented, "Not bad", "No alarm", "OK", and the participants asked which one they preferred. Four participants thought "No Alarm" was best, three participants preferred ”OK” and two participants liked ”Not bad” best.

One participant did not like any of the alternatives.

Seven participants thought a grey strike-through icon was the best option to illustrate to the user that a website does not have the desired privacy seals. Two participants preferred only the grey seal-icon. One participant did not want an icon at all.

<u>Answers to the questions posed in test 3</u>

1) Are there any differences in how users perceive blacklisting from different countries?

Yes. The participants were asked to list how serious it is to be on a blacklist from Sweden, Denmark and Slovenia. Almost all participants assigned different degrees of seriousness to blacklists in different countries:

- Swedish most serious and Slovenian least serious: 4 participants.
- Swedish most serious and the other equally serious: 3 participants.
- Swedish and Danish most serious: 2 participants.
- Slovenian most serious, followed by Danish and then Swedish: 1 participant.
- Equally serious regardless country: 2 participants.

Seven out of twelve participants thought it was most serious to be blacklisted in Sweden, followed by Denmark. Only two participants thought it was equally serious to be blacklisted regardless country.

The participants gave different comments on why the degree of seriousness differs, e.g.:

- The Swedish Consumer Agency (Konsumentverket) made it more serious since it is a government agency.
- Don't know what regulations they have in Slovenia, if they are as thorough as Sweden.

- If company was established worldwide or not. It is equally serious regardless country if they are.

The participants were also asked to list how serious it is to be on an alert list from Sweden, Denmark and Slovenia:

- Swedish most serious and Slovenian least serious: 2 participants.
- Swedish most serious and the other equally serious: 4 participants.
- Swedish and Danish most serious: 1 participant.
- Equally serious regardless country: 5 participants.

The participants were also asked to compare the seriousness of blacklist to alert list, and the result showed that five participants considered them equally serious, four participants thought that the blacklist was most serious and three participants answerer alert list.

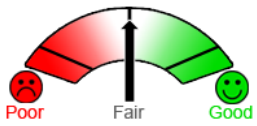
2) Is the result Fair/No alert understood by the users?

The "fair" result was not fully understood. As previously described, eight participants chose not to send data in scenario 3. The participants were later asked to explain what the "fair" result means while looking at an image of the detailed trust evaluation result. Only four participants gave a correct answer. A "fair" result was interpreted as "not evaluated" by as many as half of the participants, *"No evaluation is performed since everything is neutral…"*.

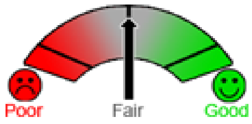
The confusion of the "fair" result can be affected by the fact that PrimeLife functions were not supported in the scenario, and there was a confusion of what it means when PrimeLife functions are not supported by a service provider, although as many as nine participants answered correct when asked if a website that doesn't support PrimeLife functions still can be evaluated (see question 4 below).

3) Which variant of trust meter do the users prefer?

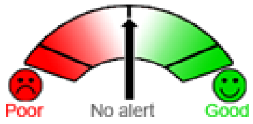
The meter itself was understood quiet well by all participants and most participants thought it was good to see the whole scale of possible results (from "Poor" to "Good").



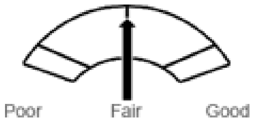
4 participants



3 participants



3 participants



1 participant

1 participant preferred the grey meter without the names (not shown here).

4) Do the users understand that a website can be evaluated even if it doesn't support PrimeLife-functions?

Yes, nine participants answered correctly. Three participants were unsure, one of them changed his/her mind during the interview and one believed that both services side were evaluated.

Other findings

When asked which side the evaluation regarded (user or services side) nine out of twelve participants answered correct. Two participants were unsure, one of which changed his mind during the interview and then gave the correct answer. The last participant thought that both sides were evaluated.

The participants were asked what would happen if they clicked on the link "security & privacy alert lists". Eight of them answered that they would get a general explanation of alert lists and four expected a list of the different alert lists. The same question was asked about the link "desired privacy seals" and half of the participants expected a general explanation while the other half expected a list of the different privacy seals. When asked the same question about the link "PrimeLife functions" all participants expected an explanation of the functions. Not all participants specified how they thought that the information would be presented but the majority emphasised that the presentation depends on much information is being presented. Two participants answered that the information could drop-down and two preferred a pop-up.

5.3 Results overview

In this section, we briefly summarise the main findings of the three test rounds.

The positive results of the usability tests can be summarised as follows:

- 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/OK/Fair"-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. This was not further evaluated in test 2 and 3.
- As many as 14 out of the 20 participants in test 1 and 2 liked the function they tested to be called "Trust Evaluation".
- All but one participant in test 1 and 2 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.
- Nearly all participants 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 mockups:

- The more detailed trust evaluation results on the second layer were harder to understand for most test persons. The most difficult evaluation result to interpret for the test participants was the detailed "Fair" evaluation result, several participants stated that the website was "not evaluated", *"No evaluation is preformed since everything is neutral…".*
- The seal icons with question marks were hard to understand for most participants. All test participants misunderstood the seal icon with an hour glass. The icon was changed to a greyed out seal with a grey line crossing it but some participants still had difficulty determining what the icon represented.

- 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*”.
- Almost all participants assigned different degrees of seriousness to blacklists in different countries. All test participants were Swedish and perceived a Swedish blacklist as the most serious one.
- There has also remained confusion for some test users on how trust evaluation can work if the services side is not PrimeLife enabled. Hence, the users need to be better informed via the interface or other means that information about the services side’s trustworthiness can mostly be obtained from third parties and do not require PrimeLife support at the services side.

Chapter 6

Related UI Approaches

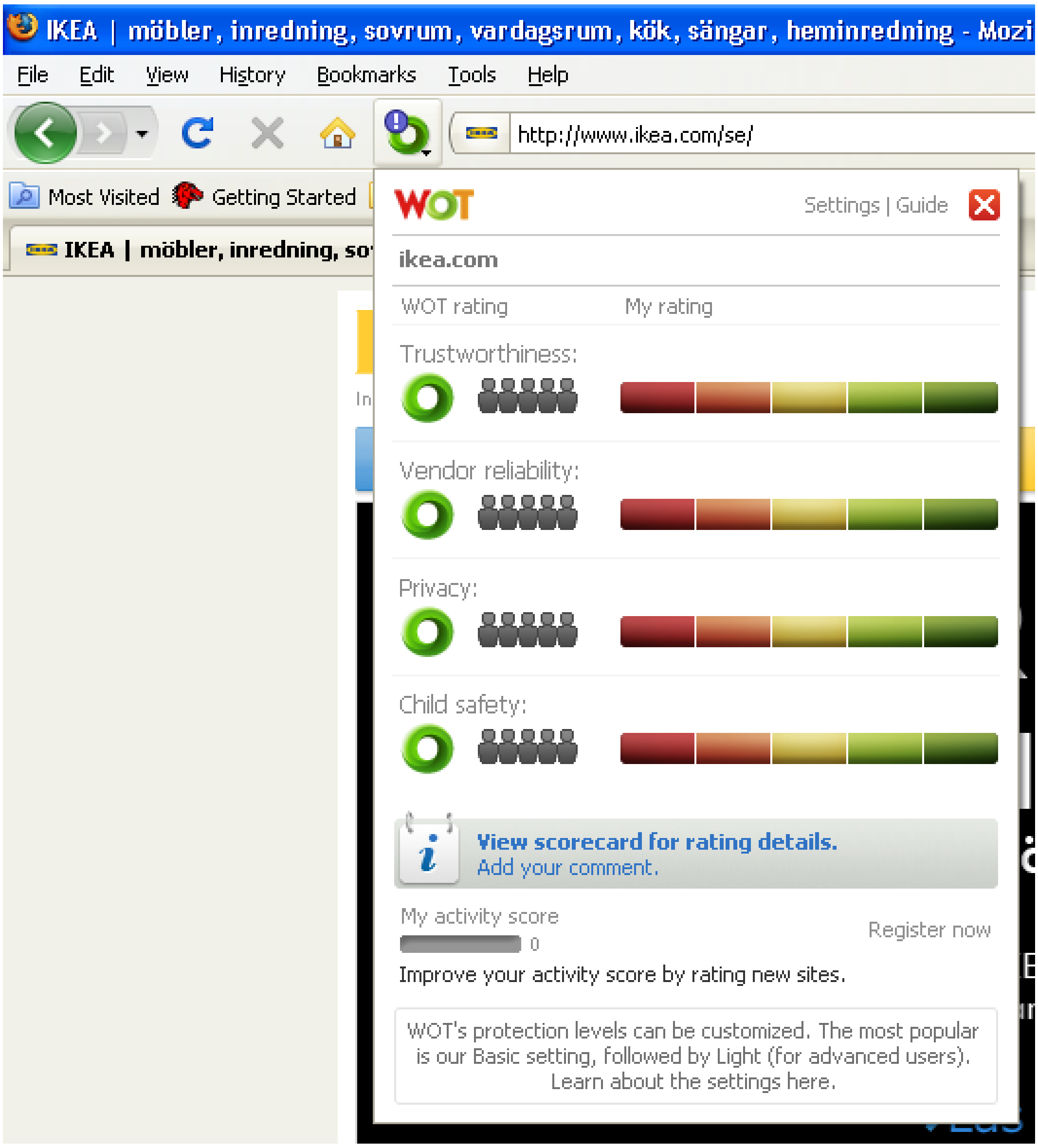
Examples for related trust evaluation functions, which both measure reputation based on user ratings, are for example WOT and TrustPlus[8] .

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 4). 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 (as something which is "ok" or something which is already symbolising weak trust properties).

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 (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 5) to symbolise trust ratings on a hierarchical scale from "do not trust" to "most trustworthy". Figure 6 shows an example of a display of a TrustPlus rating. For our purposes, however, we think that the less fine-grained scale with only three value ranges 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.

[8] http://www.trustplus.com



IKEA | möbler, inredning, sovrum, vardagsrum, kök, sängar, heminredning - Mozi

http://www.ikea.com/se/

IKEA | möbler, inredning, so

WOT Settings | Guide

ikea.com

WOT rating My rating

Trustworthiness:

Vendor reliability:

Privacy:

Child safety:

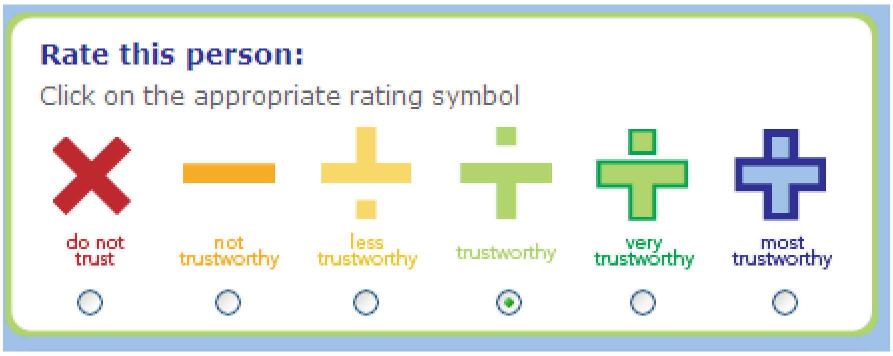
View scorecard for rating details.
Add your comment.

My activity score 0 Register now

Improve your activity score by rating new sites.

WOT's protection levels can be customized. The most popular is our Basic setting, followed by Light (for advanced users). Learn about the settings here.

Figure 4: WOT User Interface for evaluating a site through user ratings

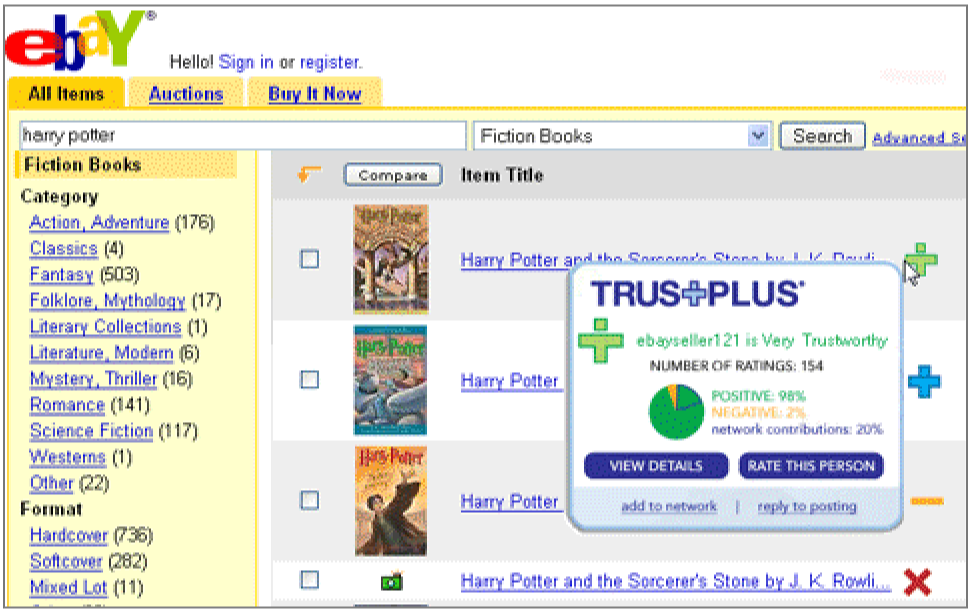


Rate this person:

Click on the appropriate rating symbol

do not trust	not trustworthy	less trustworthy	trustworthy	very trustworthy	most trustworthy
○	○	○	●	○	○

Figure 5: TrustPlus Inc. rating symbols



Fiction Books

Category

- Action, Adventure (176)
- Classics (4)
- Fantasy (503)
- Folklore, Mythology (17)
- Literary Collections (1)
- Literature, Modern (6)
- Mystery, Thriller (16)
- Romance (141)
- Science Fiction (117)
- Westerns (1)
- Other (22)

Format

- Hardcover (736)
- Softcover (282)
- Mixed Lot (11)

□ Harry Potter and the Sorcerer's Stone by J. K. Rowli...

□ Harry Potter

□ Harry Potter

□ Harry Potter and the Sorcerer's Stone by J. K. Rowli...

TRUS✚PLUS

ebayseller121 is Very Trustworthy

NUMBER OF RATINGS: 154

POSITIVE: 98%

NEGATIVE: 2%

network contributions: 20%

Figure 6: Example display of individual TrustPlus rating

Chapter 7

Conclusions and Outlook

Trust has been playing an important role in PrimeLife, because users do not only need to trust their own platforms (i.e. the user-side IDM) to manage their data accordingly but also need to trust the services sides that they process their data in a privacy-friendly and secure manner and according to the business agreements with the users.

After having investigated social trust factors for establishing reliable end user trust, we presented mockups for a Trust Evaluation Function in this deliverable, which utilises these trust factors and supports the user in reaching more informed decisions about the trustworthiness of online services.

First usability tests for three iterations of our PrimeLife trust evaluation function UI mockups clearly showed that such a trust evaluation function is much appreciated by end users. The presentation of overall evaluation results on top level as well as the fact that the services side was evaluated were well understood. Some users had problems though to understand the “neutral” evaluation result (in case a site has no seal, is not supporting PrimeLife functions, is not blacklisted and does not appear on alert lists), which we first phrased with ”Not bad”, “ok”, and then “fair”. However, in the post-test interviews, there were no clear preferences for other names (such as “No alert”). Hence, the illustration of “neutral” results is one of the most difficult issues and still needs to be investigated further.

Usability tests of the last version of the trust evaluation mockups will also be repeated at the usability lab of PrimeLife partner CURE with Austrian test users, which will allow us to do an intercultural comparison and analyse some cultural aspects of how the trust parameters are perceived.

Besides, we will also plan to extend our trust evaluation function to include reputation values of communication partners, which will allow us to evaluate not only the trustworthiness of services sides but also individual social community users. This will be based on findings of Activity 1 and WP2.2, on multilaterally secure reputation schemes and meaningful reputation aggregation mechanisms.

References

(Andersson et al. 2005) Andersson, C., Camenisch, J., Crane, S. Fischer-Hübner, S., Leenes, R., Pearson, S., Pettersson, J.S., and Sommer, D.. Trust in PRIME. Proceedings of the 5th IEEE Int. Symposium on Signal Processing and IT, December 18-21, 2005, Athens, Greece.

(Fischer-Hübner et al. 2008) Fischer-Hübner, S., Pettersson, J.S., Bergmann, M., Hansen, M., Pearson, S. Casassa-Mont, M. in: Aquisti et al. (Eds.), Digital Privacy – Theory, Technologies, and Practices, Auerbach Publications, 2008.

(Fischer-Hübner et al. 2009) Fischer-Hübner, S., Köffel, Ch., Wästlund, E., Wolkerstorfer, P.,PrimeLife HCI Research Report, Version V1, PrimeLife EU FP7 Project Deliverable D4.1.1, 26 February 2009.

(Günther and Spiekermann 2005) Günther, O. and Spiekermann, S., RFID and the perception of control: The consumer's view, in Communications of the ACM 48(9):73-76, September 2005.

(Johnston et al 2003) Johnston, J., Eloff, J. H.P. & Labuschagne, L. Security and human computer interfaces. Computers & Security, Vol. 22 (8): 675-684, 2003.

(Köffel et al. 2008) Köffel, Ch. Wästlund, E., Wolkerstorfer, P. PRIME IPv3 Usability Test Report V1.2, 25 July 2008.

(Leenes et al. 2005) Leenes, R., Lips, M., Poels, R.,Hoogwout, M. User aspects of Privacy and Identity Management in Online Environments: towardsa theoretical model of social factors. in PRIME Framework V1 (chapter 9), Editors: Fischer-Hübner, S., Andersson, Ch., Holleboom, T., PRIME project Deliverable D14.1.a, June 2005.

(Lindström 2009a) Lindström, M., Usability Test Report – Pilot Tests of Trust Evaluation (unpublished). Technical report, Karlstad University, 2009.

(Lindström 2009b) Lindström, M., Usability Test Report – Second Pilot Tests of Trust Evaluation (unpublished). Technical report, Karlstad University, 2009.

(Lindström and Nilsson 2009) Lindström, M. and Nilsson, J., Usability Test Report – Third Pilot Tests of Trust Evaluation (unpublished). Technical report, Karlstad University, 2009.

(Pearson 2006) Pearson, S., Towards Automated Evaluation of Trust Constraints, in Trust Management, LNCS 3986, Springer Berlin/Heidelberg, 252-266, 2006.

(Pettersson et al. 2005) Pettersson, J.S., Fischer-Hübner, S., Danielsson, N., Nilsson, J,. Bergmann, M., Clauß, S.. Kriegelstein, Th., & Krasemann, H. Making PRIME Usable. SOUPS 2005 Symposium on Usable Privacy and Security, Carnegie Mellon University, July 6-8 July, 2005, Pittsburgh. Available in ACM Digital Library.

(Riegelsberger et al. 2005) Riegelsberger, J., Sasse, M.A., McCarthy, J. D. The Mechanics of Trust: A Framework for Research and Design. International Journal of Human-Computer Studies, 62(3), 2005, pp.381-422.

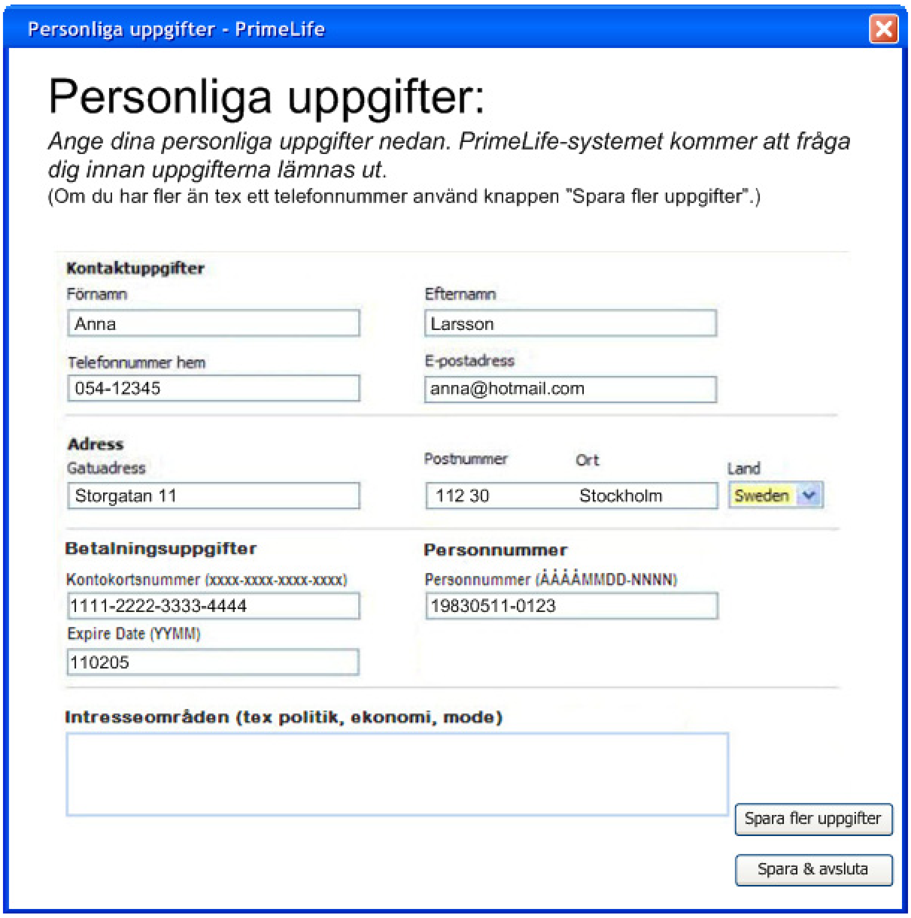
(Trustguide 2006) Lacohée, H., Crane,S., Pippen, A.,Trustguide: Final Report, October 2006.

(Turner 2001) Turner, C. W., M. Zavod & W. Yurcik, "Factors that Affect the Perception of Security and Privacy of E-commerce Web Sites". Proceedings of the Fourth International Conference on Electronic Commerce Research, Dallas TX, November 2001.

Appendix A

User Interface Prototypes Evaluated in Three Usability Test Sessions

A.1 Initial user interface used in all three tests



Personliga uppgifter:

Ange dina personliga uppgifter nedan. PrimeLife-systemet kommer att fråga dig innan uppgifterna lämnas ut.

(Om du har fler än tex ett telefonnummer använd knappen "Spara fler uppgifter".)

Kontaktuppgifter

Förnamn: Anna

Efternamn: Larsson

Telefonnummer hem: 054-12345

E-postadress: anna@hotmail.com

Adress

Gatuadress: Storgatan 11

Postnummer: 112 30

Ort: Stockholm

Land: Sweden

Betalningsuppgifter

Kontokortsnummer (xxxx-xxxx-xxxx-xxxx): 1111-2222-3333-4444

Expire Date (YYMM): 110205

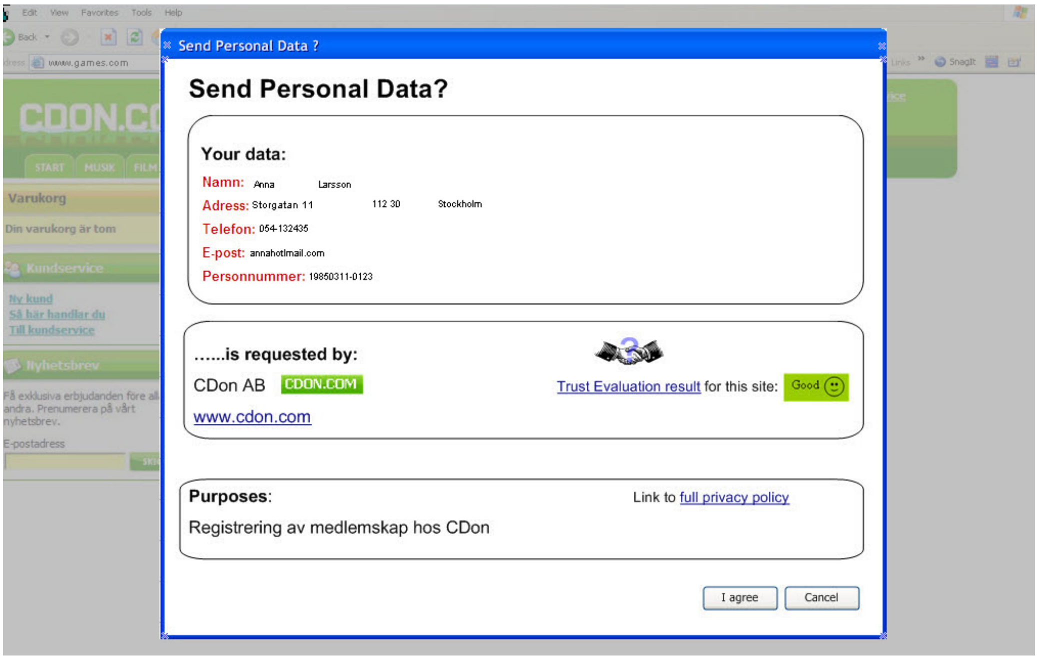
Personnummer

Personnummer (ÅÅÅÅMMDD-NNNN): 19830511-0123

Intresseområden (tex politik, ekonomi, mode)

Figure 7: UI for entering personal data (fictitious data is used), scenario group A: scenario 1

A.2 Selection of user interfaces in first test session



Send Personal Data?

Your data:

Namn: Anna Larsson

Adress: Storgatan 11 112 30 Stockholm

Telefon: 054-132435

E-post: annahotlmail.com

Personnummer: 19850311-0123

......is requested by:

CDon AB CDON.COM

Trust Evaluation result for this site: Good

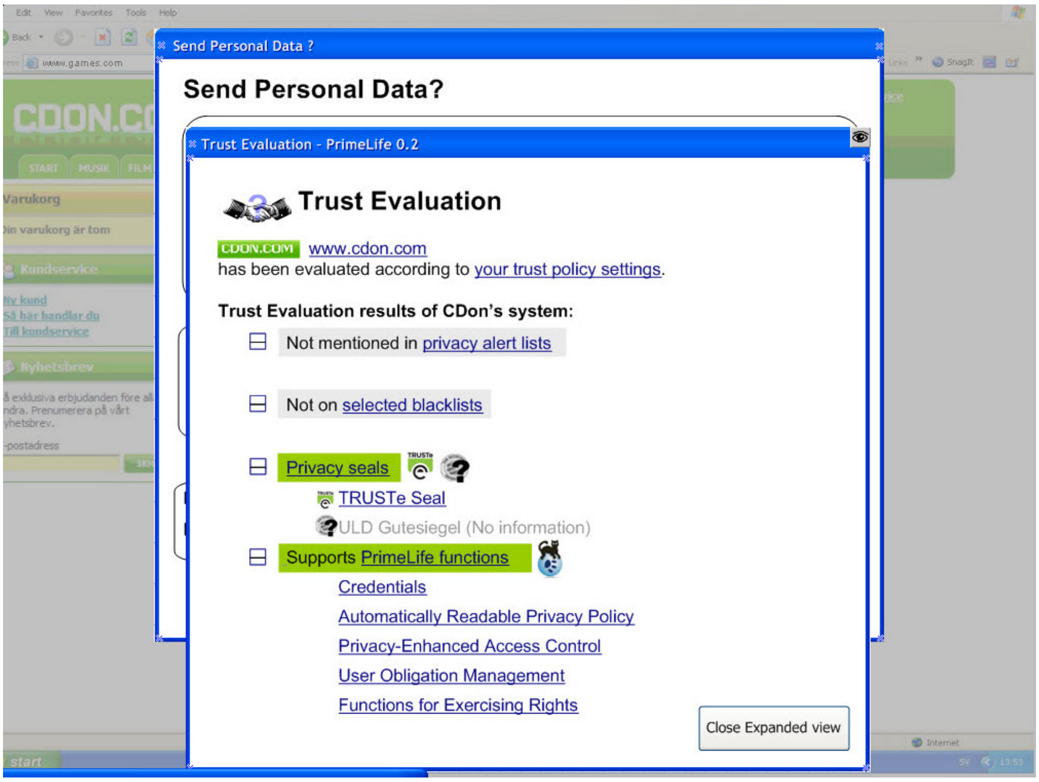
www.cdon.com

Purposes:

Link to full privacy policy

Registrering av medlemskap hos CDon

Figure 8: "Send Data" popped-up when the website requests personal data, scenario group D: scenario 2 – "good" result



Trust Evaluation

CDON.COM www.cdon.com
has been evaluated according to your trust policy settings.

Trust Evaluation results of CDon's system:

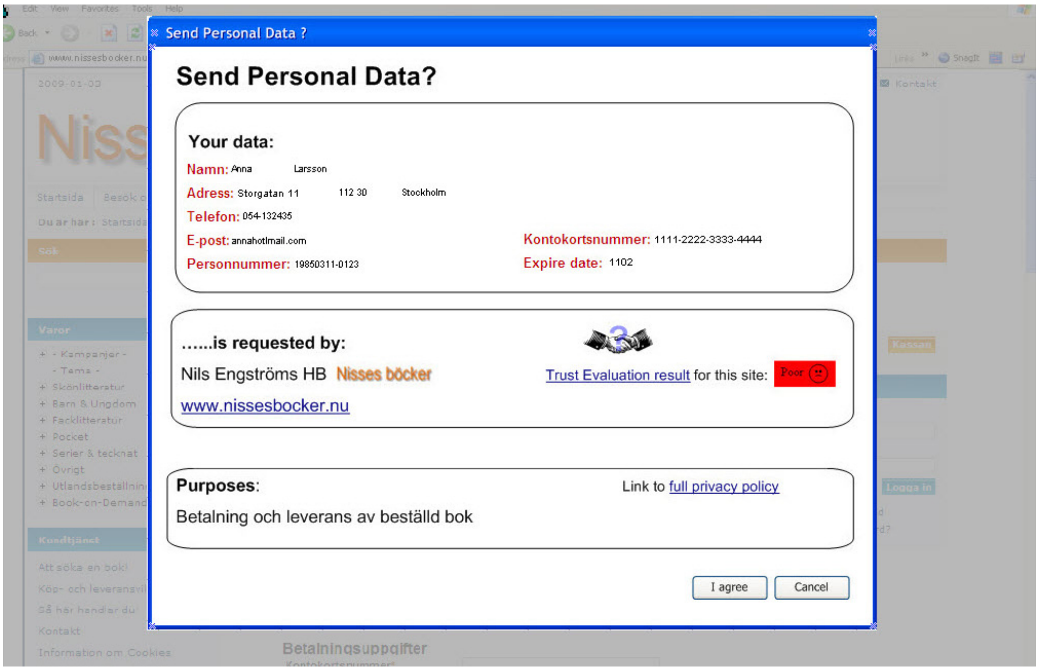
⊟ Not mentioned in privacy alert lists

⊟ Not on selected blacklists

⊟ Privacy seals
- TRUSTe Seal
- ULD Gutesiegel (No information)

⊟ Supports PrimeLife functions
- Credentials
- Automatically Readable Privacy Policy
- Privacy-Enhanced Access Control
- User Obligation Management
- Functions for Exercising Rights

Figure 9: "Expanded view" of Trust Evaluation Result in scenario group D: scenario 2


Send Personal Data ?

Send Personal Data?

Your data:

Namn: Anna Larsson

Adress: Storgatan 11 112 30 Stockholm

Telefon: 054-132435

E-post: annahotlmail.com

Personnummer: 19850311-0123

Kontokortsnummer: 1111-2222-3333-4444

Expire date: 1102

......is requested by:

Nils Engströms HB Nisses böcker

www.nissesbocker.nu

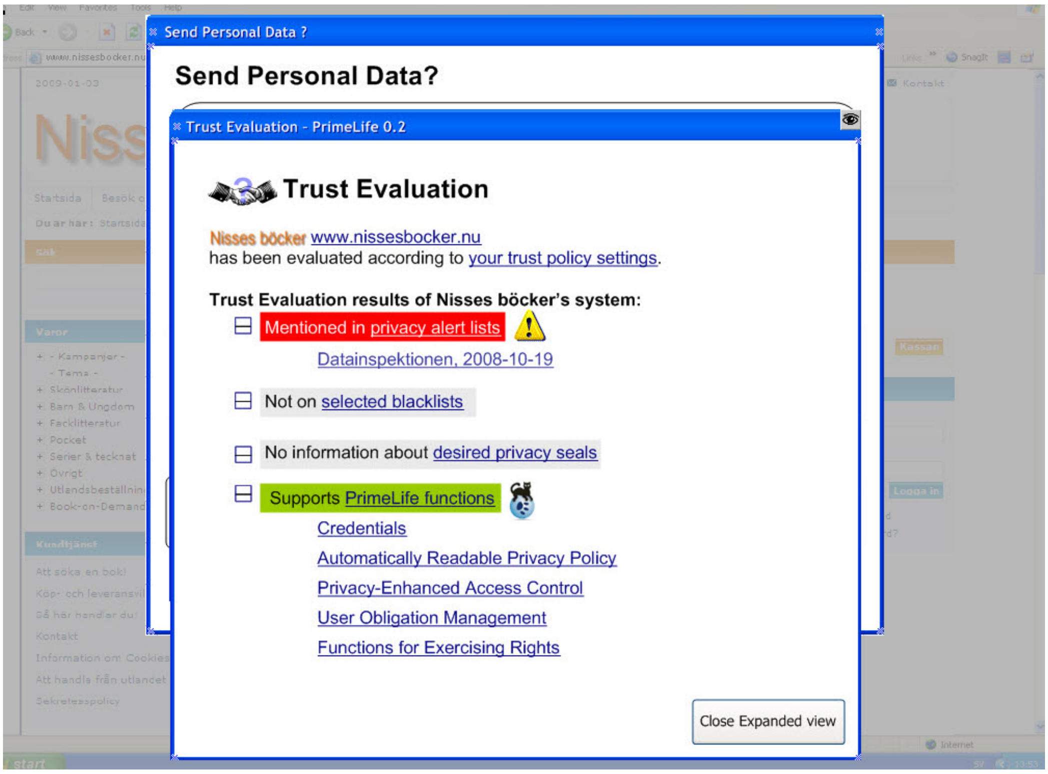
Trust Evaluation result for this site: Poor ☹

Purposes:

Betalning och leverans av beställd bok

Link to full privacy policy

Figure 10: “Send Data” has popped-up when the website requests personal data, scenario group B: scenario 3 – “poor” result


Send Personal Data ?

Send Personal Data?

Trust Evaluation - PrimeLife 0.2

Trust Evaluation

Nisses böcker www.nissesbocker.nu
has been evaluated according to your trust policy settings.

Trust Evaluation results of Nisses böcker’s system:

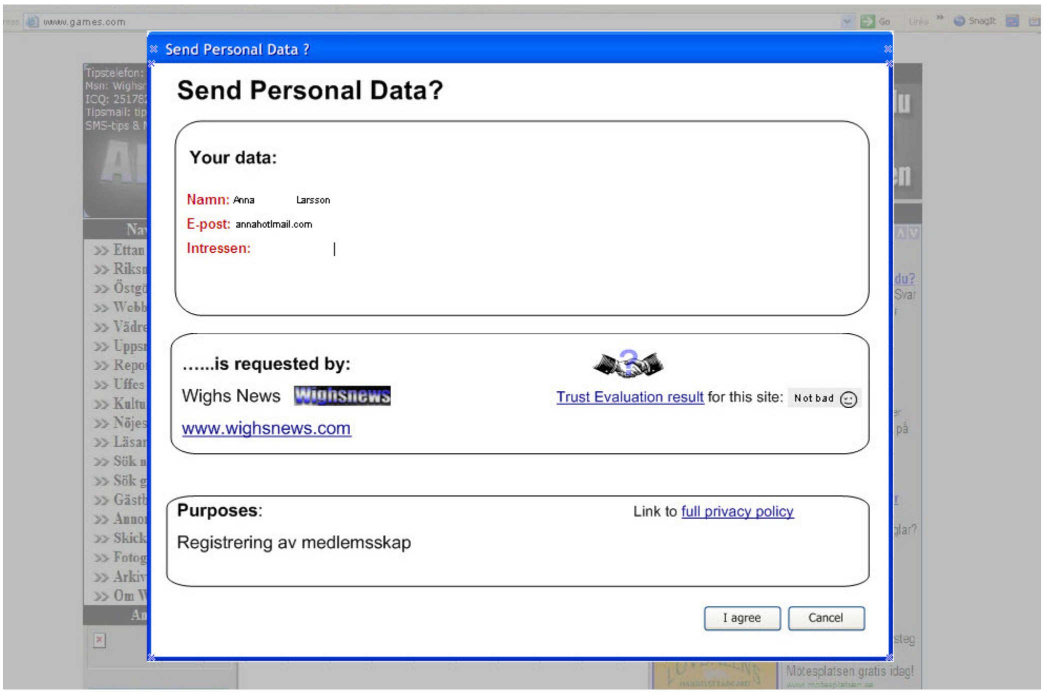
⊟ Mentioned in privacy alert lists ⚠
Datainspektionen, 2008-10-19

⊟ Not on selected blacklists

⊟ No information about desired privacy seals

⊟ Supports PrimeLife functions
Credentials
Automatically Readable Privacy Policy
Privacy-Enhanced Access Control
User Obligation Management
Functions for Exercising Rights

Figure 11: “Expanded view” of Trust Evaluation Result in scenario group B: scenario 3



Send Personal Data?

Your data:

Namn: Anna Larsson

E-post: annahotlmail.com

Intressen:

……is requested by:

Wighs News Wighsnews

www.wighsnews.com

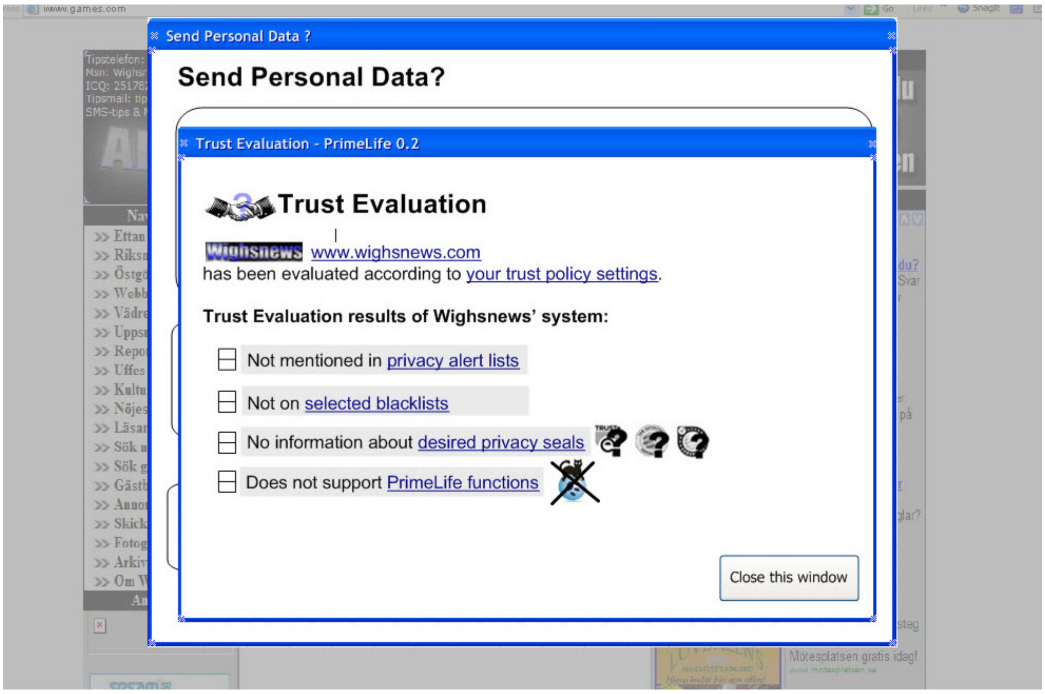
Trust Evaluation result for this site: Not bad ☺

Purposes:

Registrering av medlemsskap

Link to full privacy policy

Figure 12: “Send Data” has popped-up when the website requests personal data, scenario group C: scenario 5 – “Not bad” result



Send Personal Data?

Trust Evaluation

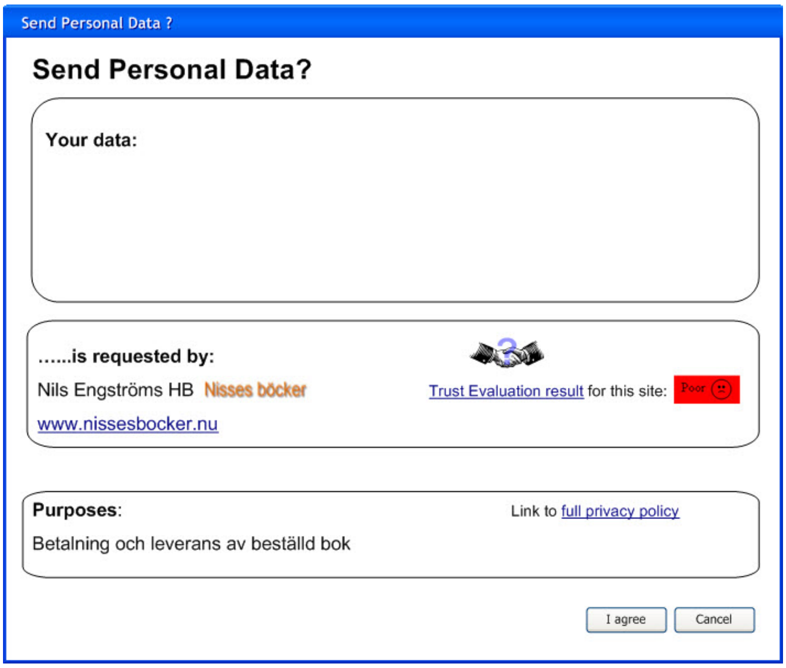
Wighsnews www.wighsnews.com has been evaluated according to your trust policy settings.

Trust Evaluation results of Wighsnews’ system:

- □ Not mentioned in privacy alert lists
- □ Not on selected blacklists
- □ No information about desired privacy seals
- □ Does not support PrimeLife functions

Figure 13: “Expanded view” of Trust Evaluation Result in scenario group C: scenario 5

A.3 User interfaces in second test session



Send Personal Data ?

Send Personal Data?

Your data:

......is requested by:

Nils Engströms HB Nisses böcker

www.nissesbocker.nu

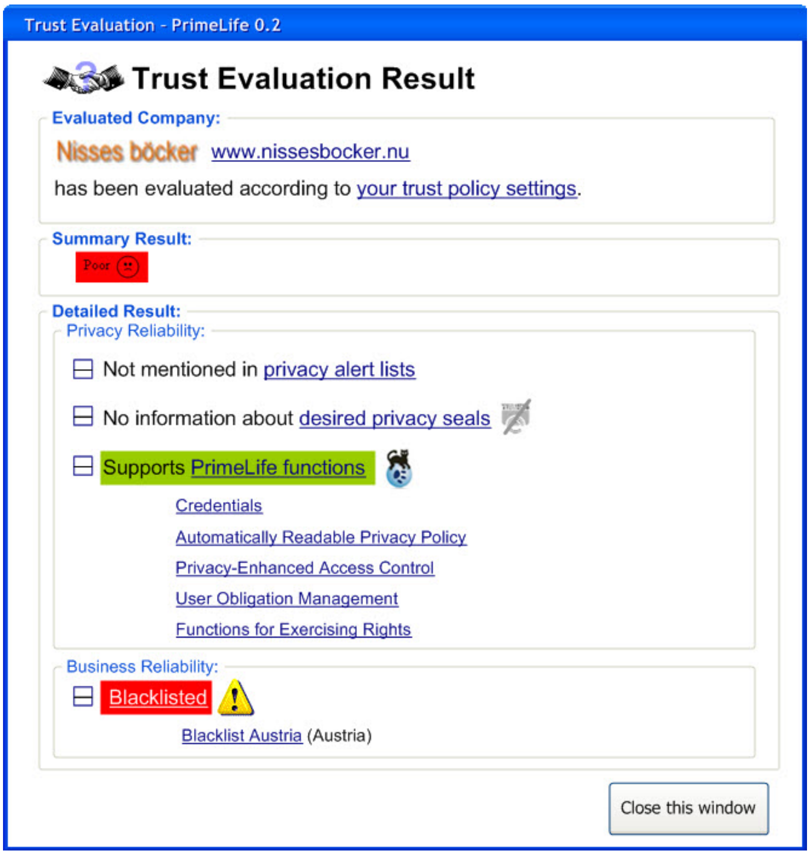
Trust Evaluation result for this site: Poor

Purposes:

Betalning och leverans av beställd bok

Link to full privacy policy

Figure 14: “Send Data” (empty) pops up when the website requests personal data, scenario group B: scenario 2 – “poor” result



Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Company:

Nisses böcker www.nissesbocker.nu

has been evaluated according to your trust policy settings.

Summary Result:

Poor

Detailed Result:

Privacy Reliability:

⊟ Not mentioned in privacy alert lists

⊟ No information about desired privacy seals

⊟ Supports PrimeLife functions

Credentials

Automatically Readable Privacy Policy

Privacy-Enhanced Access Control

User Obligation Management

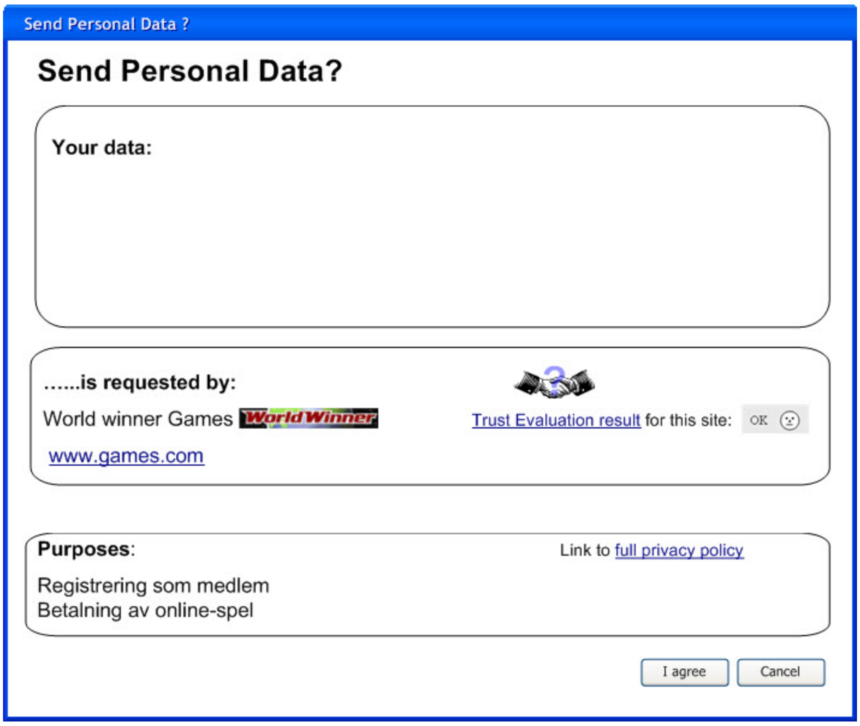
Functions for Exercising Rights

Business Reliability:

⊟ Blacklisted

Blacklist Austria (Austria)

Figure 15: “Expanded view” of Trust Evaluation Result in scenario group B: scenario 2



Send Personal Data ?

Send Personal Data?

Your data:

......is requested by:

World winner Games

www.games.com

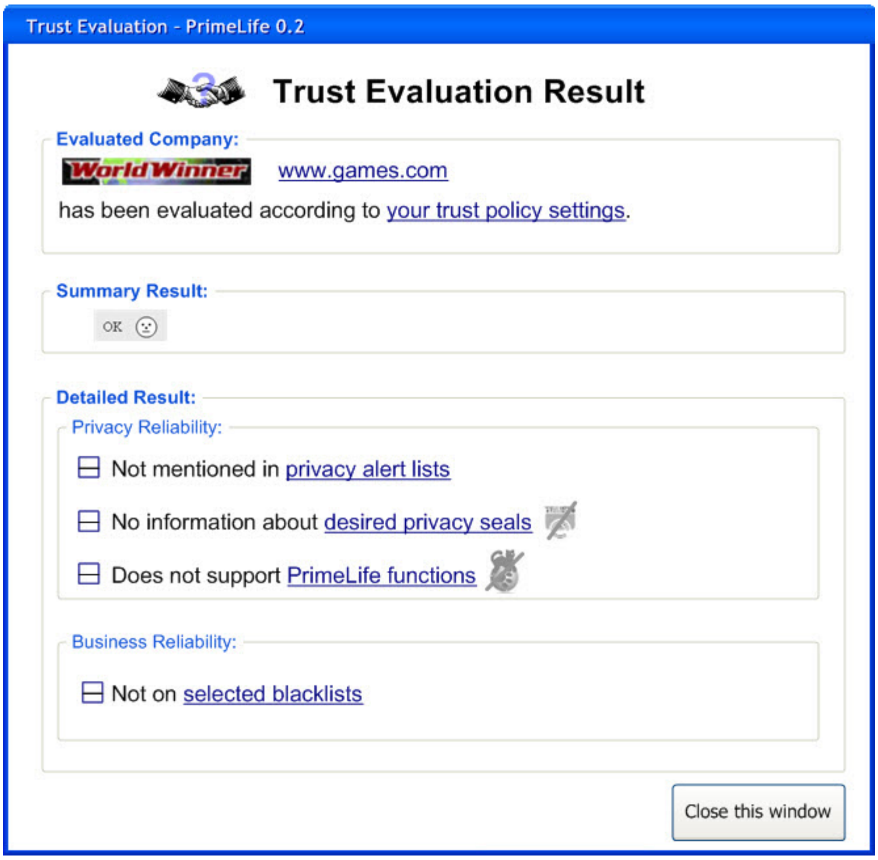
Trust Evaluation result for this site: OK ☺

Purposes:

Registrering som medlem
Betalning av online-spel

Link to full privacy policy

Figure 16: "Send Data" (empty) pops up when the website requests personal data, scenario group C: scenario 3 – "OK" result



Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Company:

www.games.com

has been evaluated according to your trust policy settings.

Summary Result:

OK ☺

Detailed Result:

Privacy Reliability:

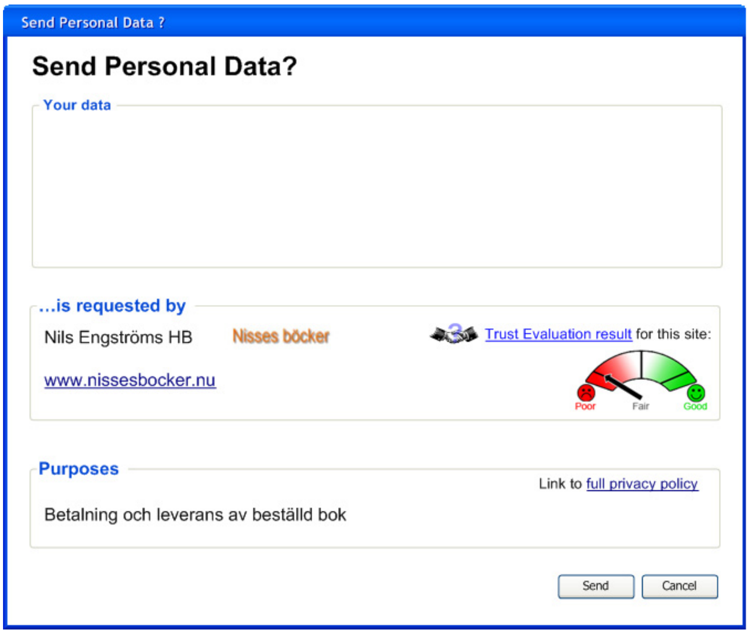
- ⊟ Not mentioned in privacy alert lists
- ⊟ No information about desired privacy seals
- ⊟ Does not support PrimeLife functions

Business Reliability:

- ⊟ Not on selected blacklists

Figure 17: "Expanded view" of Trust Evaluation Result in scenario group C: scenario 3

A.4 Selection if user interfaces in third test session



Send Personal Data ?

Send Personal Data?

Your data

...is requested by

Nils Engströms HB Nisses böcker

www.nissesbocker.nu

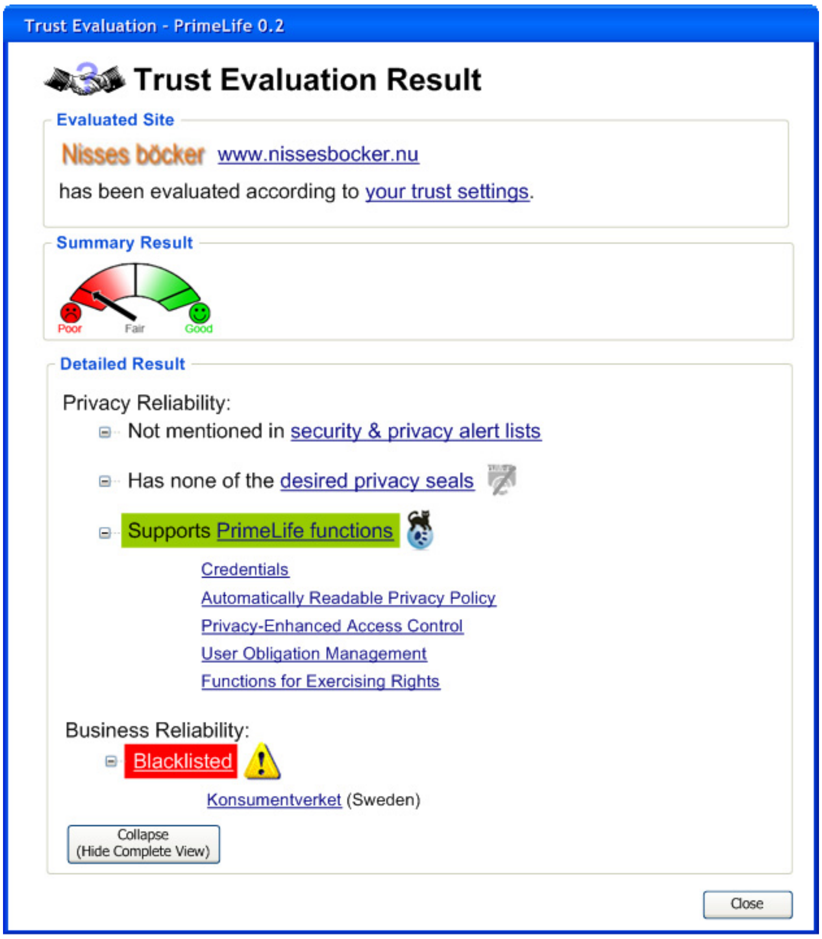
Trust Evaluation result for this site:

Purposes

Link to full privacy policy

Betalning och leverans av beställd bok

Figure 18: “Send Data” (empty) pops up when the website requests personal data, scenario group B: scenario 2 – “Poor” result



Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Site

Nisses böcker www.nissesbocker.nu

has been evaluated according to your trust settings.

Summary Result

Detailed Result

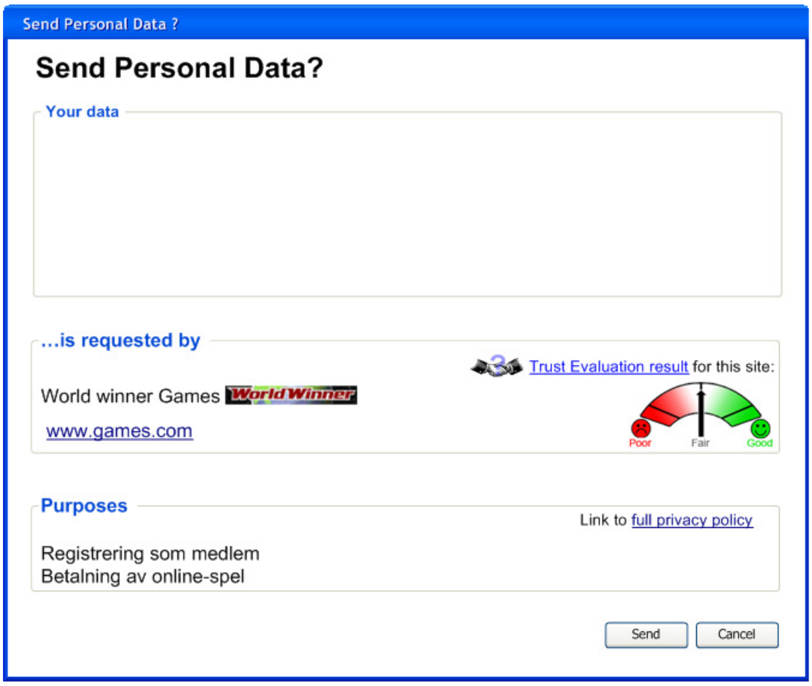
Privacy Reliability:

- Not mentioned in security & privacy alert lists
- Has none of the desired privacy seals
- Supports PrimeLife functions
  - Credentials
  - Automatically Readable Privacy Policy
  - Privacy-Enhanced Access Control
  - User Obligation Management
  - Functions for Exercising Rights

Business Reliability:

- Blacklisted
  - Konsumentverket (Sweden)

Figure 19: “Expanded view” of Trust Evaluation Result in scenario group B: scenario 2



Send Personal Data ?

Send Personal Data?

Your data

...is requested by

Trust Evaluation result for this site:

World winner Games

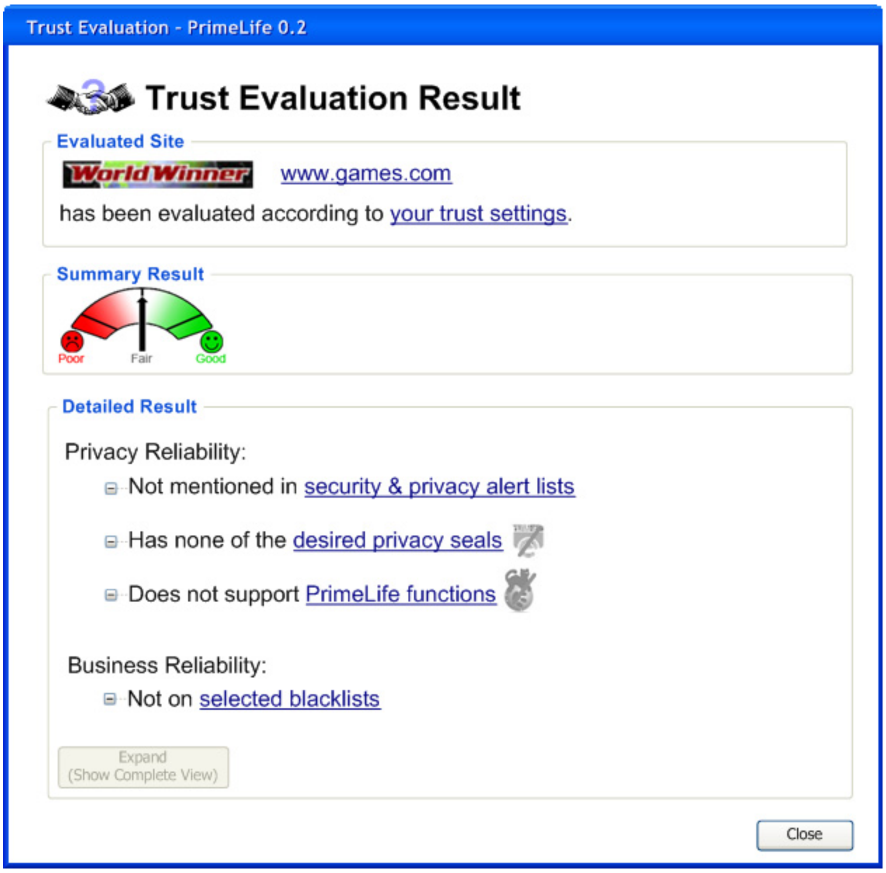
www.games.com

Purposes

Link to full privacy policy

Registrering som medlem
Betalning av online-spel

Figure 20: “Send Data” (empty) pops up when the website requests personal data, scenario group C: scenario 3 – “Fair” result



Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Site

www.games.com

has been evaluated according to your trust settings.

Summary Result

Detailed Result

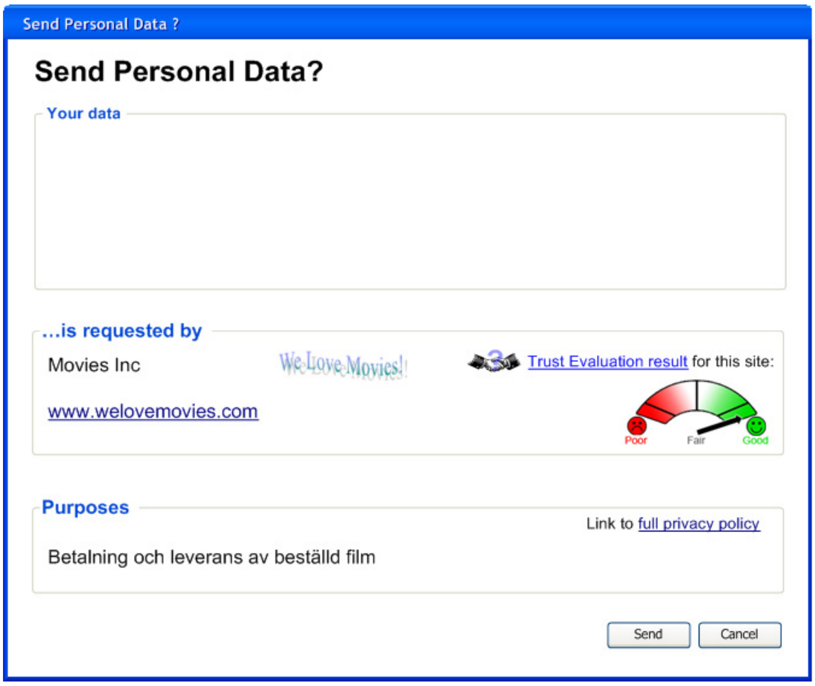
Privacy Reliability:

- Not mentioned in security & privacy alert lists
- Has none of the desired privacy seals
- Does not support PrimeLife functions

Business Reliability:

- Not on selected blacklists

Figure 21: “Expanded view” of Trust Evaluation Result in scenario group C: scenario 3



Send Personal Data ?

Send Personal Data?

Your data

...is requested by

Movies Inc

www.welovemovies.com

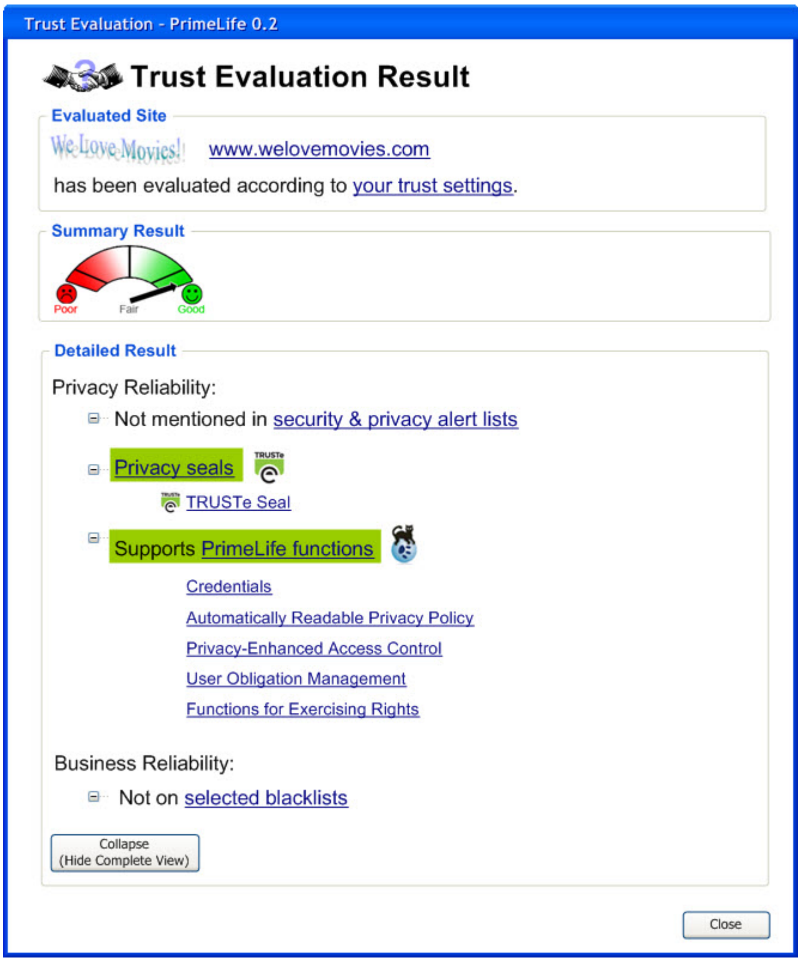
Trust Evaluation result for this site:

Purposes

Link to full privacy policy

Betalning och leverans av beställd film

Figure 22: "Send Data" (empty) pops up when the website requests personal data, scenario group D: scenario 4 – "Fair" result



Trust Evaluation - PrimeLife 0.2

Trust Evaluation Result

Evaluated Site

www.welovemovies.com

has been evaluated according to your trust settings.

Summary Result

Detailed Result

Privacy Reliability:

- Not mentioned in security & privacy alert lists
- Privacy seals
  - TRUSTe Seal
- Supports PrimeLife functions
  - Credentials
  - Automatically Readable Privacy Policy
  - Privacy-Enhanced Access Control
  - User Obligation Management
  - Functions for Exercising Rights

Business Reliability:

- Not on selected blacklists

Figure 23: "Expanded view" of Trust Evaluation Result in scenario group D: scenario 4