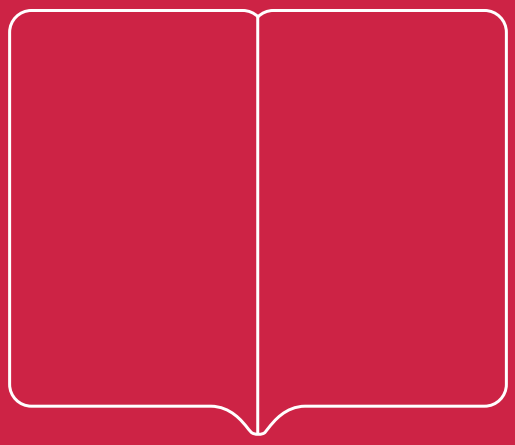
Addressing societal concerns on legal and privacy issues in ICT-related projects

Trustworthy ICT Research in Europe for ICT Security Industry, ICT Security Users and Researchers

Addressing societal concerns on legal and privacy issues in ICT-related projects

Trustworthy ICT Research in Europe for ICT Security Industry, ICT Security Users and Researchers

Table of Contents



Executive Summary

This deliverable presents a map of the social barriers to ICT adoption in the domain of security- and privacy-related solutions. The wider goal in connection to the FIRE project is

- to provide a better understanding of these barriers to adoption;
- to inform the industry and the researchers about the possible reasons why some technologies may fail to enter the market;
- to enable this knowledge to be taken into account in developing and assessing various future R&D activities.

The results were obtained by a qualitative coding of 11 projects (mainly FP7 Trust and Security, CIP ICT Policy Support Programme): ACTIBIO, AVANTSSAR, ECRN, PICOS, PoSecCo, PRIMELIFE, SecureSCM, SHIELDS, TAS3, UaESMC and UTRUSTit. The projects were chosen according to their proximity to actual use experience: actual implementation experience was prioritized over interviews with users and other similar methods which, in turn, was prioritized over expert assessments about users' needs and wants.
Seven main types of barriers were detected:

- exclusion of end-users from development;
- incompatibility with the existing user context;
- the adoption entailing too much uncertainty;
- no perceived need for the technology;
- insufficient communication;
- lack of usability;
- lack of trust.

These barriers are co-dependent and shape each other (e.g. in some cases enhanced usability might increase trust in the product/service). Additionally it was also observed that trust-enhancing technologies themselves seemed to suffer from the lack of trust. Therefore, a view that there is a 'technological fix' to trust-related issues should be avoided as it is too narrow and unrealistic: simultaneous changes in technological, economic, political, legal and cultural domains across multiple institutional levels are required instead to increase collective trust.

Based on this mapping six suggestions are made to reduce social barriers to privacy/ security-related ICT adoption in medium and long term. The results also inform the overall cluster strategy development (deliverable D4.3):

- Industry: there is no single recipe to facilitate the adoption process. A customized approach is needed in each case.
- Industry-science interaction: sociological knowledge about the evolution of technological artefacts and systems should be integrated into the development of new products.
- Industry-science interaction: the attempts to reduce social barriers to privacy/security-related ICTs should be based on explicit considerations of the phase of development of the technologies in question.

- Industry-science interaction: the industry needs to approach the researchers (of the social) with specific questions in mind in order to ensure the co-evolution of theories of technological dynamics and the integration of this knowledge into product development.
- Science: further research on ICTs and trust is needed.
- European Commission: future project proposals should contain sections explicitly outlining reasons whether and why user involvement would be considered necessary (or not).

Introduction

This document is deliverable D6.1 of a project Facilitate Industry and Research in Europe (FIRE), a Coordination and Support Action project under Call FP7-ICT-2011-8 of the ICT Work Program 2011/12. Full information on this project, including the contents of this deliverable, is available online at

http://www.trustworthyictonfire.com

The aim of this deliverable is to present a map of social barriers to ICT adoption in the domain of security- and privacy-related solutions. The wider goal in connection to the FIRE project is to provide a better understanding of the barriers to adoption, to inform the industry and the researchers about the possible reasons why some technologies may fail to enter the market and to enable this knowledge to be taken into account in developing and assessing various future R&D activities. The output of this deliverable also informs the overall cluster strategy development (D4.3). The results themselves were obtained by a qualitative coding of selected projects (mainly FP7 Trust and Security; CIP ICT Policy Support Programme).

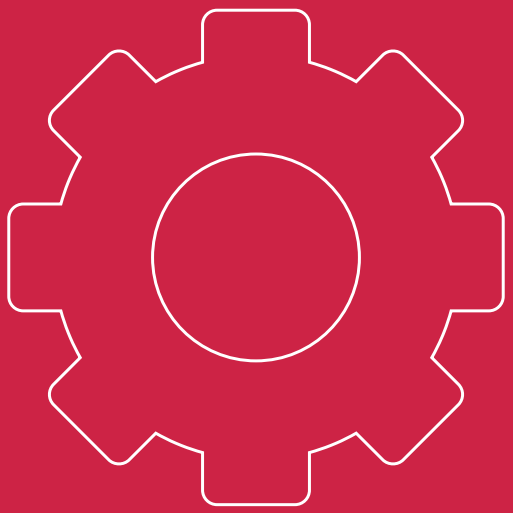
The first part of the report presents the methodological principles of case selection (which projects were selected and why) as well as the rationale of the qualitative coding process itself. The second part outlines the map of identified problems, discussing each of the seven main barriers to adoption along with empirical examples. The third part briefly reflects on the limitations of the method, summarizes the main findings, highlights the possible avenues of future research and provides suggestions for reducing these barriers in the medium and long term.

2.1 Project description

The FIRE project will provide a strategic approach, organizational support and network capability for researchers, technology developers, consultants, system integrators and governments to improve their European co-operation by addressing challenges in the current fragmented landscape. The project will facilitate information security companies to improve take-up of European Trustworthy ICT research, and also enable researchers to connect and exploit their technology solutions with the information security technology companies, systems integrators and end users. The project will also contribute to aligning European Trustworthy ICT research with specific market sector requirements for exploitation. The project will be able to support coordination by developing pan-EU cluster strategy and research agendas/roadmaps in key research areas. FIRE will impact and improve most importantly the European industrial competitiveness in markets of trustworthy ICT.

2.2 Objectives of the deliverable

- To provide an overview of the social barriers to privacy/security-related ICT adoption;
- To discuss addressing societal concerns on legal and privacy issues in ICT-related projects;
- To provide suggestions for reducing social barriers to adoption in the medium and long term.



Methodology

The overall goal of this deliverable is to outline the social barriers to the adoption of privacy- and security-related ICT solutions. The term 'social' is defined residually, i.e. it involves every factor potentially affecting user adoption that is not related to the internal technical characteristics and features of the technology. By this definition, in a situation in which a technology is well-functioning from an engineering point of view but might nevertheless be resisted by users, one is dealing with an impact of a social barrier.

3.1 Case selection principles

The case selection proceeded in two rounds. In the first one the formal criteria of inclusion were defined in order to make the scope of the research manageable. As a result the cases were selected as follows (in decreasing order of importance):

- FP7 Trust and Security projects;
- CIP ICT Policy Support Programme projects;
- Other privacy/security-related FP7 projects (obtained my manually reviewing the project descriptions).

The total amount of cases thus selected was 110.

In the second round further case selection was performed on substantive grounds. The projects in which there was evidence of direct user involvement (e.g. laboratory tests, on-site trials etc.) were ascribed primary importance. However, in some cases there was no direct user involvement although the users were consulted about their needs and wants. Finally, in some cases the experts, not the end-users themselves, were asked to assess the market potential of the technologies and to highlight the possible barriers to adoption. All these cases were included to the coding process (see the following section).

In general terms the substantive case selection reflects the preference of

- actual implementation experience over;
- the users' best guesses about their future use experience over;
- the experts' guesses about the users' guesses about the future use experience of the latter.

In other words, the decisive criterion of substantive case selection was the proximity to the actual user experience. It was assumed that direct user experience can reveal various factors that the developers (or the users themselves) might have downplayed or failed to consider at all prior to the implementation. Therefore, direct user involvement was assumed to reflect the real-life constraints to ICT adoption most accurately.

The implications of these methodological choices are fourfold:

- the developers' own ideas about users' potential experience (materialized in formal devices such as personas, use scenarios etc.) were excluded regardless the claims made by the developers (e.g. the insistence that the personas were 'realistic');
- formal legal and ethical analyses preceding the implementation were also excluded;
- the cases in which the enterprises themselves comprised the group of end-users were included;
- the coding had to be restricted to cases in which the information about the use experience was already present (i.e. cases in which user trials were planned but had not been carried out yet had to be excluded).

Qualitative open coding was chosen as the best method to approach the task. Essentially the technique can be described as a structured yet flexible classification process which continues to develop constantly as the research progresses further. The aim is to build a hierarchy of codes out of scattered remarks on social barriers found in various project deliverables.

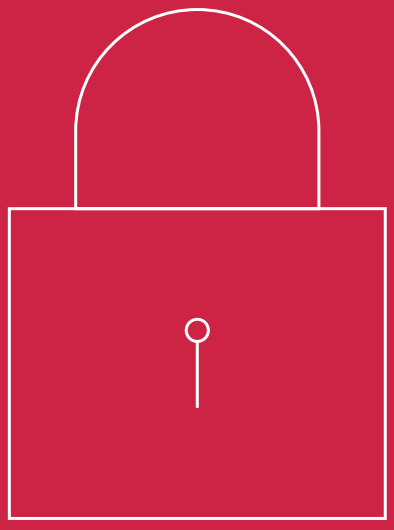
3.2 Coding process description

Qualitative open coding is particularly suitable in cases where the range of potential barriers is not known in advance and the aim is to locate the relevant barriers, not to quantify them. The reason is simple: if the amount of knowledge about the studied phenomenon is limited it is best to avoid formulating specific hypotheses early on as these may contain arbitrary and non-significant factors reflecting the implicit presumptions of the analyst. This, however, may lead to 'analytical blinkers' which prevent the researcher from detecting important factors and bias him/her to focus on a few selected ones (i.e. to perform confirmatory research). But if the analytical focus is on locating all potentially relevant factors this is clearly an inappropriate research strategy. Qualitative open coding enables to avoid these pitfalls. In this particular deliverable the principles of qualitative open coding were applied as follows:

- according to the above formal and substantive case selection criteria (see the previous section) the relevant cases were chosen;
- subsequently deliverables with sections related to assessing user experience were located;
- various text extracts highlighting different issues with user adoption were coded using NVivo software as free nodes (i.e. the text extracts were classified as instances of a more general problem);

- those free nodes operating on various level of abstraction were gradually assembled into a hierarchy of nodes in which some problems (sub-codes) could be seen as instances of more general barriers to adoption (main codes);
- at the same time the less relevant nodes or nodes that were duplicating each other in content were merged or deleted altogether.

As an end result, the unstructured textual descriptions contained in various project deliverables could be systematized into a relatively structured map of barriers to adoption defined by general overarching themes. This is presented in the following section.



Privacy- and security-related ict solutions: (potential) barriers to adoption

This chapter presents an overview of the barriers to adoption of privacy/security-related ICT technologies. First, a brief overview of each coded case is provided. The following section describes general overarching themes, highlights the more specific barriers corresponding to each theme and brings examples from coded projects. Note that since some of the barriers were not derived from an actual implementation experience but from the user or expert assessments (e.g. interviews, surveys) not all of them may necessarily realize: hence the bracketed word 'potential' in the chapter title.

3.2 Overview of coded cases

The number of cases on which relevant information corresponding to the case selection criteria (see section 1.1) could be found was 11. What follows is a brief description of each case. These summaries are abbreviated versions of the publicly available project descriptions.

ACTIBIO (Unobtrusive authentication using activity related and soft biometrics) aims to develop a completely new concept in biometric authentication: the extraction of multi-modal biometric signatures based on the response of the user to specific stimuli, while performing specific but natural work-related activities. The novelty of the approach lies in the fact that the biometric measurements will correspond to the response of the person to specific events being however, fully unobtrusive and fully integrated in an Ambient Intelligence infrastructure.

AVANTSSAR (Automated validation of trust and security of service-oriented architectures) proposes a rigorous technology to validate both the service components and their composition into secure service architectures.

ECRN (European Civil Registry Network) establishes a secure and certified electronic infrastructure that will allow Civil Acts Registrars in different countries to exchange information on Civil Act certificates (birth, death, marriage, divorce). The pilot was started in four countries (Italy, Belgium, Germany and the Netherlands).

PICOS (Privacy and identity management for community services) aims to develop a state-of-the-art platform for providing the trust, privacy and identity management aspects of community services and applications on the Internet and in mobile communication networks

PoSecCo (Policy and Security Configuration Management) aims to overcome the service providers' trade-off between profitability and security/compliance by establishing a traceable and sustainable link between high-level requirements and low-level configuration settings. Substantial improvements are expected in the areas of policy modeling and conflict detection across architectural layers, decision support for policy refinement processes, policy and configuration

change management including validation, remediation and audit support, and security management processes in Future Internet application scenarios.

PRIMELIFE (Privacy and identity management in Europe for life) aims to offer tools for protecting privacy in emerging Internet applications such as collaborative scenarios and virtual communities, and for maintaining life-long privacy. Its long-term vision is to counter the trend to life-long personal data trails data without compromising on functionality.

SecureSCM (Secure supply chain management) proposes to use secure computation to overcome data sharing risks in supply chain management and enable the secure collaboration and interoperation of supply chain partners to gain the advantages of knowledge-based collaborative supply chain planning, forecasting, benchmarking and management.

SHIELDS (Detecting known security vulnerabilities from within design and development tools) aims to increase software security by bridging the gap between security experts and software practitioners and by providing the software developers with the means to effectively prevent occurrences of known vulnerabilities when building software.

TAS3 (Trusted architecture for securely shared services) proposes an Integrated Project that will develop and implement an architecture with trusted services to manage and process distributed personal information. The personal information that will be processed and managed can consist of any type of information that is owned by or refers to people.

UaESMC (Usable and Efficient Secure Multiparty Computation) aims to bring the techniques and tools for Secure Multiparty Computation (SMC) to a level where they can be applied to decisional and computational problems of practical size in several different social and economic sectors. The project will combine the identification of a representative set of computational problems, the development of appropriate cryptographic and other tools for solving those problems in a privacy-preserving manner, the study of incentives of various parties to participate in privacy-preserving computations, and the exploration of practical limits and trade-offs in the deployment of SMC solutions.

UTRUSTit (Usable TRUST in the Internet of Things) focuses on integrating the user directly in the trust chain, guaranteeing transparency in the underlying security and reliability properties of the IoT. The results of uTRUSTit enable system manufacturers and system integrators to express the underlying security concepts to users in a comprehensible way, allowing them to make valid judgements on the trustworthiness of such systems.

4.2 Overview of the main barriers to adoption

The main barriers to the adoption of privacy/security-related ICTs can be classified into 7 + 1 types: exclusion of end-users from development, incompatibility with the existing user context, the adoption entailing too much uncertainty, no perceived need for technology, insufficient communication, lack of usability, lack of trust and a residual category containing various barriers. Figure 1 (see the next page) provides a visual summary of these barriers.

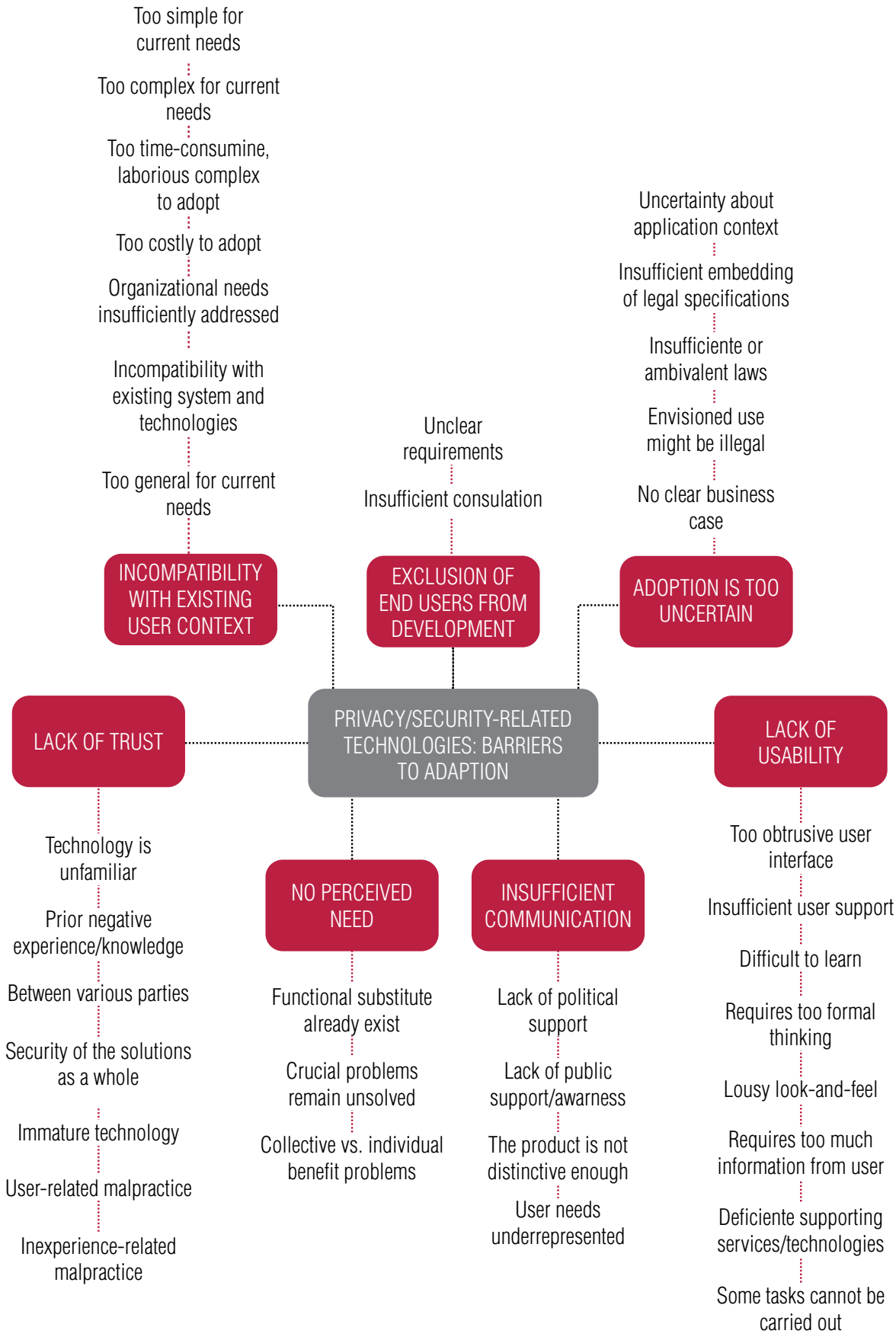

PRIVACY/SECURITY-RELATED TECHNOLOGIES: BARRIERS TO ADAPTION
INCOMPATIBILITY WITH EXISTING USER CONTEXT
Too simple for current needs
Too complex for current needs
Too time-consumine, laborious complex to adopt
Too costly to adopt
Organizational needs insufficiently addressed
Incompatibility with existing system and technologies
Too general for current needs
EXCLUSION OF END USERS FROM DEVELOPMENT
Unclear requirements
Insufficient consulation
ADOPTION IS TOO UNCERTAIN
Uncertainty about application context
Insufficient embedding of legal specifications
Insufficiente or ambivalent laws
Envisioned use might be illegal
No clear business case
LACK OF TRUST
Technology is unfamiliar
Prior negative experience/knowledge
Between various parties
Security of the solutions as a whole
Immature technology
User-related malpractice
Inexperience-related malpractice
NO PERCEIVED NEED
Functional substitute already exist
Crucial problems remain unsolved
Collective vs. individual benefit problems
INSUFFICIENT COMMUNICATION
Lack of political support
Lack of public support/awarness
The product is not distinctive enough
User needs underrepresented
LACK OF USABILITY
Too obtrusive user interface
Insufficient user support
Difficult to learn
Requires too formal thinking
Lousy look-and-feel
Requires too much information from user
Deficiente supporting services/technologies
Some tasks cannot be carried out

Figure 1

4.2.1 Exclusion of end-users from development

In this case the development process has suffered from a supply-side bias: the developer has set the agenda – the problem to be solved – and has focused on developing the technological devices to overcome this problem. At the same time it is uncertain to what extent this agenda is shared by the future users. In other words,

- user requirements have remained unclear or underspecified;
- users have been insufficiently consulted about the technological choices made by the developers.

Example: TAS3 (Trusted Architecture for Securely Shared Services) project instantiated its developed architecture in the domains of employability and e-health for trial purposes. Potential users themselves were involved in various ways, e.g. surveys, lab tests, workshops and live demonstrations. It was observed that some of the features did not fully match user requirements and the users occasionally needed to resort to workarounds. In this particular case the insufficient specification of user requirements was amplified by the fact that the users were excluded from participating in many choices made at the development level.

4.2.2 Incompatibility with the existing user context

Contrary to the previous category in this one the user needs may be well-articulated and the users may be willing to adopt the technology. However, this willingness may only be theoretical because of numerous obstacles related to the existing technological, organizational and institutional context that threaten to slow the adoption process down to the point of impracticality. The following barriers were detected:

- the implementation requires too much time and effort, is too complex;
- the implementation focuses on technological possibilities omitting the organizational needs;
- the costs of adoption are too high;
- the solution is incompatible with existing systems and technologies (e.g. business frameworks, organization's planning tools);
- technology may be too complex for current needs;
- technology may lack certain crucial functions desired by the user;
- technology may be too general for current needs.

Examples: UaESMC (Usable and Efficient Secure Multiparty Computation) project aims to make the relevant SMC techniques and tools practically applicable in various domains (industries, universities, public sector etc.). In order to probe the feasibility of this endeavour, including the potential barriers, a number of interviews were conducted with specialists from many fields. One of the interviewees pointed out that the implementation of SMC techniques

would require new types of legal contracts between parties thereby increasing the cost of adoption. It was also argued that for a variety of enterprises the level of security offered by SMC is unnecessarily high and thus the solution itself too complex.

The high cost and complexity of adoption were recurring themes in many cases (e.g. ACTIBIO, AVANTSSAR, SHIELDS). Sometimes a clash between theory and practice was explicitly mentioned: an example is provided by the SecureSCM (Secury Supply Chain Management) project which aims to employ secure computation techniques to facilitate collaborative supply chain management and planning, thereby reducing overall costs. A number of expert interviews were conducted to assess the feasibility of some SecureSCM use cases. It was pointed out that although the approach might be hypothetically useful the long-term planning would be far too complex if all supply chain partners were to be involved.

While the issues of complexity, cost and unnecessary or deficient functionality are easy to understand, the case of ACTIBIO provides an additional nuance. Essentially the project set out to develop unobtrusive biometric authentication techniques. The review of public perception of biometrics identified the problem that the technology may be too general: for example, the fingerprints of persons with certain types of skin (dry, older) cannot be identified properly, some people have amputated limbs, some may be too tall or short falling outside the 'normal' parameters of the system. In other words, general-purpose authentication techniques, if designed with insufficient sensitivity to these issues, may end up discriminating against certain 'non-standard' user groups.

4.2.3 The adoption entails too much uncertainty

In this category the user needs may be well-articulated but the users hesitate to adopt the technology because of various uncertainties and potential obstacles that may arise in the adoption process. These risks may be manifested in various contexts (e.g. economic or legal):

- legal specifications are insufficiently embedded into the technology;
- the intended use of the new technology might be illegal;
- existing legal context is insufficient or ambivalent;
- it is unclear how exactly (in what conditions and for what purposes) the technology is to be applied;
- here is no example of successful use, no clear business case.

Examples: the purpose of the SHIELDS project was to provide software developers with means to prevent various vulnerabilities during the process of software-creation. Although the preliminary evaluation results were by and large positive the project report points out that as SHIELDS is at the early stage of development then the possible return on investment is difficult to assess.

This indicates a more general issue shared by other cases (UaESMC, SecureSCM): the way in which the enterprises can use new technologies in order to increase their profits is far from clear. In other words, a clear business case is often missing. The cases indicated that the reasons for this might be many, e.g. the added value is unclear, it is not known whether the general tool can be successfully customized to industry-specific needs or the successful precedent of use may be simply lacking. However, the insistence on a latter may lead to a self-fulfilling vicious circle: lack of a clear exemplary use case resulting in a collective wait-and-see attitude of the enterprises thus decreasing the possibilities to realize such a case in the first place.

4.2.4 No perceived need for the technology

In this particular case the users see no need to deviate from the existing solutions and associated practices as their needs are already being served well enough. Once again this situation may emerge for different reasons:

- sufficient functional substitute to the new technology already exists;
- the technology does not help to solve the problems deemed crucial by the user;
- collective efficiency does not necessarily translate into an individual one.

Examples: while assessing the market potential of SecureSCM one of the experts argued that whereas such a centralized collaborative planning may indeed increase the overall efficiency of the supply chain, this is not necessarily true for every participating organization. In other words, some enterprises may benefit from the existing information asymmetry. Thus the alleged 'efficiency' of the new technologies is actually socially contested and the willingness of the users to adopt new technologies intimately related to the features of an existing social context.

In the UaESMC case, however, the root cause of the lack of need is somewhat different. Here the experts observed that scientists and statistical offices often need to have a full overview of the data in order to assess its quality or to be able to combine different databases according to an agreed set of standards. In other words, in these cases SMC techniques would simply not help to solve the problems relevant to the user and thus the technology would not be adopted.

4.2.5 Insufficient communication

This category describes the potential barriers arising from the lack of communication. In other words, the technological solution may well address existing user needs but the developers and the potential users have yet to establish a direct connection. Alternatively, the wider diffusion may require gaining support from various stakeholders. Therefore, the problems pertaining to communication issues are as follows:

- lack of political support;
- lack of public support, public awareness;
- the distinctiveness of the new technology from its alternatives has been insufficiently stressed;
- representation of technological aspects dominates over the consideration of user needs.

Examples: various problems pertaining to communication were addressed in the UAESMC project. Interviewees argued that unless the presentation of SMC issues to the private sector is simple enough for the non-experts to grasp, the technology would not be adopted. Consequently the project report concludes that communicative effort should be put into conveying the messages of trustworthiness, monitoring and auditing to the target audiences. In other words, addressing user needs should take precedence over the stress on novel technological possibilities. The SHIELDS project report added an additional aspect by observing that the brand of the product would need further development in order to achieve sufficient market differentiation.

4.2.6 Lack of usability

This theme unites various factors that influence different dimensions of the usability of the technology, i.e. learnability, understandability, operability and attractiveness. The number of these issues is large, they are often technology-specific and presumably can often be quickly corrected in the design process. Therefore, only a selection of observed issues are noted here:

- lack of help/support, insufficient documentation;
- information overflow leading to difficulties with learning to use the technology;
- too much information is required from the user;
- too formal thinking is required from the user;
- the look-and-feel of the user interface leaves something to be desired;
- the user interface seems too obtrusive;
- some tasks are difficult to carry out or cannot be carried out at all;
- supporting services and/or technologies are deficient masking the usability of the focal technology.

Examples: AVANTSSAR (Automated validation of trust and security of service-oriented architectures) aims to offer usable and efficient tools and techniques for various industry and standardization organizations so the development of new network and service infrastructures could be accelerated and their security/robustness enhanced. The tools were tried out in four different organizational settings. Part of the overall process involved the formal modelling of various actual systems. It was found that the system developer is facing an interpretive barrier: the developer's view of the system is much more specific than the

output of the AVANTSSAR tools. Thus shifting between different levels of abstraction is required to translate the formally detected vulnerabilities to the actual features of the real system. This, however, increases the cognitive load of the developer and may therefore negatively influence the usability of the AVANTSSAR tools.

PICOS (Privacy and identity management for community services) project on the other hand assessed the usability of its trust and identity management tools with two groups (anglers and gamers) in lab and in real-life settings employing both quantitative and qualitative methods. The user trials revealed numerous little shortcomings: some participants could not find all useful functions, the feedback about the results of the actions of the user was insufficient, some messages popped up often enough to become obtrusive, some features seemed too complex etc. etc. Similar little deficiencies regarding learnability, support and look-and-feel were also encountered in other cases such as PoSecCo, PRIMELIFE, SHIELDS and TAS3.

4.2.7 Lack of trust

This is another major category which contains a wide variety of different reasons why the users may hesitate to adopt the technology even if they perceive it as potentially beneficial. Similarly to the category of usability, the number of these issues is large with many reasons being technology-specific. However, it is unclear whether the issue of trust can be overcome as quickly and efficiently as that of usability. Some of the observed issues are:

- the technology is considered immature;
- user-related malpractice may compromise the overall security of the system;
- inexperience-related malpractice may compromise the overall security of the system;
- the technological solution is unfamiliar, the working principle is not understood;
- various parties do not trust each other (e.g. the perceived insecurity of government databases, distrust towards service providers);
- prior negative experience affects trust towards new technologies;
- security of the solution as a whole is uncertain.

Examples: uTRUSTit (Usable TRUST in the Internet of Things) aims to make the information security properties of the Internet of Things more transparent to the end-user. The stated purpose is to integrate the user directly in the trust chain, allowing the users to make valid judgments about the trustworthiness of various systems. Part of the evaluation of the prototype (Trust Feedback Toolkit) focused on the determinants of trust. Among other findings it was shown that the fulfilment of the task (or the lack of it), users' experience with certain tasks and the content of the feedback affect perceived trust.

It appears that the presence of a new technology seems to have little impact on behaviour if trust between various parties is missing. For example, in the PICOS project one of the functionalities allowed the person to leave the community without leaving any personal traces. However, the feature was mostly not employed by the users as the latter were highly sceptical about the community service provider's willingness to actually withdraw such data. In yet another case, SecureSCM, the willingness of partners to share sensitive data was highlighted as a potential obstacle. The need for a neutral party guaranteeing the reliability of the solution and taking responsibility for errors was seen as one possible solution.

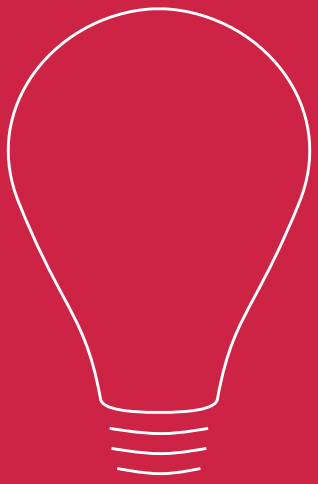
4.2.8 Other barriers

Two types of other barriers were mentioned that could hinder the adoption of privacy/security-related ICT solutions:

- potential invasion of privacy;
- new technologies might pose a health hazard.

Example: both of these barriers were raised regarding the use of biometric authentication in the ACTIBIO project. The first concerns the fear that the information obtained by biometric authentication could be misused. Increasing clarity about the laws and rules relating to data storage and the type of information to be stored was advised as a solution. This could also be seen as a special case of the presence of legal ambiguity.

The potential hazards of biometric authentication to health (e.g. iris scanners) were also noted. As most of these fears are arguably not grounded in empirical evidence this barrier might be seen as a special case of insufficient communication.



Discussion and Conclusions

5.1 Limitations of the method

Although it was argued in the first chapter that qualitative coding is a highly suitable method for mapping exercises because it offers a structured yet flexible way to deal with the research object the boundaries of which cannot be determined exactly during data collection, this method also has its shortcomings. In the following four such shortcomings will be briefly discussed in increasing order of importance.

First, the number of cases on which relevant information satisfying the case selection criteria presented in chapter one could be found was relatively small (11 or 10% of the overall cases). The situation is explained by two factors: either direct end-user involvement was not part of the project plan at all or the project had not simply entered this particular phase at the time of writing. This, however, is relatively unproblematic since a qualitative study is information-rich by definition. In other words, using a qualitative approach, even a small number of cases usually yield enough information that is generalizable to other similar cases. Moreover, it is sensible to presume that once the projects which did not involve direct end-user involvement would start to do so in the future then roughly the same types of barriers to adoption will become salient.

Second, the mapping of barriers on qualitative grounds does not enable one to assess the severity of each of these other than on a very indirect and approximate basis. Further work needs to be conducted in order to be able to say whether there are more critical problems shared by most of these privacy- and security-related technologies that would need to be addressed to accelerate the adoption process or whether a case-by-case approach would be more suitable.

Third, in order not to narrow down the case pool too much, projects in which user/expert information was sought for prior to implementation were also included. However, similarly to developers, the cognitive capacities of end-users and experts are also bounded (although they are somewhat more knowledgeable about the actual context of use). Therefore, the current results may be subject at least to three different kinds of biases: the degree to which the users are able to express their preferences (i.e. their clarity and specificity) might differ, the preferences may change in time (e.g. after adoption) (Stewart & Williams 2005) and the users may fail to foresee every important barrier (i.e. the actual adoption could entail more or different problems than assumed beforehand).

Finally, the mapping relies entirely on secondary data. That means that the information available to the researcher has already been filtered by the project participants. This may lead to a situation in which some relevant barriers are neglected or the importance of some of them is being downplayed. Moreover, the external assessment of the projects means that the participants are

explicitly motivated to retrospectively rationalize their behaviour and to avoid noting any large-scale failures even if they actually occur. A multi-level and multi-site ethnographic approach turning attention to the evolving 'biography' of artefacts or systems (Williams & Pollock 2012) would be much more preferable in order to avoid relying too much on the claims of the project participants (and end-users, for that matter).

Drawing on the foregoing analysis three main conclusions can be presented.

5.2 Summary of the main findings

1. The seven main barriers to the adoption of privacy/security-related ICT technologies are

- exclusion of end-users from development;
- incompatibility with the existing user context;
- the adoption entailing too much uncertainty;
- no perceived need for the technology;
- insufficient communication;
- lack of usability;
- lack of trust

2. These barriers are co-dependent and mutually shape each other.
Although the purpose of this mapping exercise was not to establish causal connections between the barriers it is worth noting that the latter are not independent of each other. For example, in the TAS3 project (see also section 2.7) a survey was carried out in order to detect the determinants of trust. It was found that the reliability and availability of a service, its usability, its look-and-feel and perceived security affect the trust perception. In other words, overcoming the usability-related barriers can also lead to increasing the trust of the end-users. Similarly, a high perceived need may at least temporarily reduce the importance of potential usability issues. More work could be done to explore the direction of impact and the relative importance of each of these factors.

3. There is no 'technological fix' for security/privacy/trust issues. It is curious to note that one of the main problems characteristic to the projects united under the 'Trust and Security' label still seems to be the lack of trust towards the very technologies that are meant to overcome such issues in the first place. The most anecdotal example would be the AVANTSSAR project where one of the project participants refused to implement the technology for trial purposes on the grounds that the solution was arguably too immature and incompatible with the organization's own planning tools. However, the relatively technology-centred focus of most of the projects seems to imply an implicit belief in the efficacy of a 'technological fix', that is, the idea "that ICT straightforwardly fixes a large number of existing problems in society" (van Dijk 2010: 6).

The weaknesses of this view are many: 1) it only focuses on one particular, usually beneficial effect of the technology thus excluding other possible consequences; 2) it downplays or excludes the importance of organizational and political support measures in ensuring that the problem in focus will be solved (van Dijk 2010: 11, see the same document for more ICT-related examples); 3) it underestimates the interests and capabilities of existing influential actors to maintain the status quo (i.e. to block the entry of new technologies, at least in the short term). As a result it offers a narrow and unrealistic view of technological diffusion and adoption, grossly overestimating the importance of new technologies for solving various social problems with deep-rooted causes (see section 2.4 for one of such examples). Hence it is safe to say that the actual adoption will likely require simultaneous changes in technological, economic, political, legal and cultural domains across multiple institutional levels, and will be fraught with conflict, struggle and resistance, not all of which can be presumed to be caused by ignorance or irrationality of the actors concerned.

5.3 Recommendations for further research and addressing the social barriers

The final section is concerned with outlining the implications of the findings of this deliverable for facilitating the development and take-up of privacy/security-related ICT solutions. The first part briefly touches upon the possibilities to build on the mapping as presented in this deliverable. The second part is wider in scope and aims to offer some suggestions for addressing social barriers more effectively in the medium and long term.

First, the above research can be substantially improved by focusing on the following aspects:

- To include more cases in order to expand and refine the typology.
- Subsequently the research could be taken on the next level by locating the critical problems, assessing their relative strengths and detecting the causal influence between the barriers.
- The practitioners are unlikely to be surprised by the majority of the above findings: after all, the issues of usability or the failure to consider the context of use have been recurring themes addressed over decades in the fields of Science and Technology Studies, Social Informatics, and Human-computer Interaction. Therefore, it might be useful to shift the analytical focus and ask why, despite all the apparent advances in detecting and dealing with user requirements, similar barriers to adoption continue to emerge? Are the majority of the flaws simply minor now, are we dealing with some fundamental limits to foresight or have the practitioners simply become far more attentive to 'failures', however the latter are defined?

Moving beyond the immediate focus of this deliverable six more general recommendations can be made to improve addressing the social aspects of privacy/security-related ICT solutions. Three of them are directed to the industry (1), the European Commission (5) and the scientific community (6) respectively, whereas the rest (2-4) concern the industry-research interaction.

1. There is no single recipe to facilitate the adoption process. A customized approach is needed in each case. Even the relatively small selection of cases observed and analysed in this deliverable yielded a substantial variation in terms of the scope of the project, commercial maturity, technological maturity,

overall function(s), intended context of use etc. etc. Therefore, it would be naïve, simplistic and at times counter-productive to make suggestions in the vein 'users need to be included in each case to facilitate the adoption'. The meaningfulness of various strategies for overcoming different barriers actually depends on many factors (such as the phase of development of the technological field in question) and thus specific strategies should be devised for dealing with each technology separately.

2. Sociological knowledge about the evolution of technological artefacts and systems should be integrated into the development of new products. It is notable that whereas various techniques of user involvement were enthusiastically used in the projects the discussion about the appropriateness of these techniques lacked references to the social context of their deployment. In other words, the deployment of various techniques such as usability trials or technology assessment should be coupled with sociological consideration of how particular technologies in particular socio-technical contexts tend to evolve. This issue becomes highly relevant when one moves from assessing whether a certain technique has been employed sufficiently rigorously to questioning the meaningfulness of applying these techniques in the first place (see the following point for some examples). In the long term the take-up of privacy/security-related ICTs can only be enhanced with a thorough understanding of the underlying developmental dynamics of technologies.

An interdisciplinary field of Science and Technology Studies (STS) has been devoted to exploring the dynamics of various technologies across various contexts for decades (see Russell & Williams 2002 for a somewhat dated yet comprehensive overview of the field). A recurrent finding is that the dynamics of technology are very different depending on the maturity of the technology itself, the existence of competing alternatives, the existence of and perceived problems with incumbent solutions, macro-level changes etc. (Tushman & Rosenkopf 1992, Rip & Kemp 1998). For example, if there is no dominant design for a given product class and thus the 'era of ferment' is still ongoing (Tushman & Rosenkopf 1992) usability trials may even turn out to be harmful as they are biased towards incremental refinement and tend to focus on the limitations, not on the promises of the technology (Buxton & Greenberg 2008). STS and other related fields (Social Informatics, Human-computer Interaction etc.) are well-positioned to set the agenda for assessing the overall socio-technical context and thus the appropriateness of applying various techniques to reduce or to overcome social barriers to adoption.

3. The attempts to reduce social barriers to privacy/security-related ICTs should be based on explicit considerations of the phase of development of the technologies in question. If the dynamics of technology differ from one phase to another then it is sensible to presume that the appropriate measures to facilitate the development and adoption of ICT solutions should also vary accordingly. In other words,

depending on the particular phase of development different barriers become relevant and therefore different strategies should be considered. Four context-dependent possibilities can be briefly sketched out here to illustrate the idea:

- It was observed above that high usability does not equal high usefulness. Therefore, if the maturity of the technology is low, its exact functionality, intended user context and user preferences unclear, the focus on usability is best avoided. Moreover, if the best design is yet to emerge and the impact of the technology uncertain there is little at stake for developers to organize workshops for mutual learning, sharing the knowledge and aligning the visions (Rip & te Kulve 2008). In these conditions continuing on the path of local separate technological experimentation might be best for a while until the results begin to show some promise of wider applicability.
- However, if the participants are already motivated enough to invest into organizing mutual interaction but otherwise there is still high degree of uncertainty about the dominant design, social acceptance, legal environment etc. then shifting the attention to co-constructing the mutual expectations regarding technological opportunities and user needs might be the most suitable way to proceed. Constructive Technology Assessment (Schot & Rip 1997), an approach that explicitly includes the theoretical lessons of the dynamics of technology into its framework, has been developed to meet this challenge. Lately successful applications of the principles of CTA have been made in the domain of nanotechnology (e.g. van Merkerk & Smits 2008, Rip & te Kulve 2008) demonstrating the viability of the approach. In this phase the main focus of activities is likely to move from purely technical experimentation to creating shared visions, networking and reducing ambiguity, e.g. lobbying for a favourable institutional framework which would enable the market to prosper (Raven & Geels 2010).
- It is only when the technological domain has become stabilized and the market sufficiently matured when the shift to even more specific barriers can be made. Here various issues such as designing according to explicitly expressed user preferences, fitting the product to various organizational contexts or increasing the usability of the products might become the most important activities.
- Finally, it may be that the technology as well as its socio-technical context have matured enough to achieve wider market penetration. However, the users or potentially affected groups may have been insufficiently informed, misinformed or not informed at all (see sections 2.2.5 and 2.2.8 for examples). In this situation better mapping of use domains, user preferences and the extent of impact or raising the awareness of the public by various means (e.g. popularizing articles in media, exhibitions) would be the most useful activities to be undertaken. An example of such a strategy is provided by ACTIBIO project which has explicitly aimed to target both the scientific community and the general public to facilitate the acceptance of biometric technologies.

4. The industry needs to approach the researchers (of the social) with specific questions in mind in order to ensure the co-evolution of theories of technological dynamics and the integration of this knowledge into product development. At this moment STS is characterized by an immense variety in terms of analytical focuses and research contexts. While this has served to demonstrate the general validity of some ideas it has also contributed to the somewhat fragmented nature of the domain itself. In other words, while stimulating ideas and exploratory research abound, systematic bodies of work testing very specific claims across various contexts are often incomplete or missing altogether (see the critique from Geels 2007, Wyatt & Balmer 2007).

This issue might be resolved if the industry approached the researchers (sociologists of technology) with quite particular and specific problem agendas. This would stimulate the researchers to refine the existing theories, to locate gaps in knowledge, to define the boundary conditions of their theories and to think more about the practical implications of their findings. This enhanced knowledge can then be employed in product development. Thereby the industry's problem-led agenda setting can act to stimulate industrial and scientific co-evolution.

5. Future project proposals should contain sections explicitly outlining reasons whether and why user involvement would be considered necessary (or not). It is a personal observation of the author of this deliverable that 'user involvement' has recently become a fashionable topic. It is not at all far-fetched to conclude that phrases such as this are being rhetorically employed in various project proposals to appeal to the evaluators. At the same time, the actual 'social dimension' may be peripheral to the project's core objectives and may be seen as an inconvenient add-on rather than an integral part of the project. However, in line with the above discussion the need to consider the social dimension is context-dependent: sometimes the technologies may well be too immature for extensive user involvement to make any sense. Moreover, placing too much stress on the user-side may sometimes lead to a situation in which the user preferences are well-considered but the product itself far too expensive and unable to compete on the market. As both of these situations essentially amount to a wasteful use of human and financial resources a balanced view of the interests and needs of various stakeholders should be preferred.

Therefore, in order to avoid rhetorical appeals to user involvement, to ensure the development of practicable products and to reduce the possible evaluation bias towards projects that stress the 'social dimension' it is advised that future project proposals should include sections explicitly arguing why user involvement would or would not be necessary in this particular case. Ideally, the lack of a 'social dimension' should not impact the evaluation if the corresponding argument stands on solid ground. To achieve that, however, various aspects covered in previous points should be taken into account.

6. Further research on ICTs and trust is needed. Although trust and ICTs is a topic that has certainly garnered some attention (see Paterson et al. 2008 and Robert et al. 2009 for some examples) the lack of trust still keeps emerging as one of the major barriers to adoption. This indicates that either our understanding of ICT-related trust issues is still incomplete or the cross-fertilization between scientific findings and product development is yet to happen. Moreover, it is ironic to note that the lack of trust seems to be a barrier for the very technologies meant to enhance trust in the first place. As noted in section 5.2 this only illustrates the limited viability of a 'technological fix' approach. More research is needed in order to explore the determinants of trust on various levels (from individual to cultural), to work out various trust-enhancing measures in various societal domains (technological, economic, political, legal, cultural etc.) and to combine them appropriately.

It is suggested not to view trust as a property of single products/services but as as a property of socio-technical systems as a whole (including elements such as inter-linked products/services, service providers, end-users' perceptions, underlying infrastructure, supporting products/services, legal environment, informal rules and practices etc. etc.). This wider focus would enable to move beyond specific problems new technologies are supposed to solve and instead to observe whether the socio-technical context of these technologies is favourable to facilitate diffusion of specific products/services on mass scale. It would also facilitate turning more attention to creating favourable macro-level (state, EU, international) conditions to enhance collective trust (e.g. a coordinated adoption of privacy-by-design principles).

Bibliography

I ACTIBIO *(Unobtrusive authentication using activity related and soft biometrics). 2011. D8.2, Public Perception of Surveillance Technologies. Available online* http://www.actibio.eu:8080/actibio/index.html

http://www.actibio.eu:8080/actibio/files/document/Deliverables/ACTIBIO_Deliverable_8.2.pdf

II AVANTSSAR *(Automated validation of trust and security of service-oriented architectures)*. 2011.03.01. D6.2.3, *Migration to industrial development environments: lessons learned and best practices.* Available online http://www.avantssar.eu/pdf/deliverables/avantssar-d6-2-3.pdf

III Geels, F. W. 2007b. Feelings of Discontent and the Promise of Middle Range Theory for STS: Examples from Technology Dynamics. *Science, Technology, & Human Values 32* (6): 627-651.

IV Greenberg, S., and Buxton, B. 2008.04.05-10. Usability Evaluation Considered Harmful (Some of the Time). *CHI 2008 Proceedings.*

V Van Merkerk, R. O., and Smits, R. E. H. M. 2008. Tailoring CTA for Emerging Technologies. *Technological Forecasting & Social Change 75 (3)*: 312-333.

VI Paterson, I., Maguire, H., and Al-Hakim, L. 2008. Analysing trust as a means of improving the effectiveness of the virtual supply chain. *International Journal of Networking and Virtual Organisations* 5 (3-4): 325-348.

VII PICOS (Privacy and identity management for community services). 2011.13.05. D8.3, *Final Evalutation* Report. Available online: http://www.picos-project.eu/fileadmin/user_upload/fmgr/Deliverables/WP8_Evaluation/D8.3_Final_Evaluation_Report/PICOS_D8_3_Final_Evaluation_Final_v1.pdf

VIII PRIMELIFE *(Privacy and Identity Management in Europe for Life).* 2011.20.05. D4.1.5, Final HCI Research Report. Available online: http://primelife.ercim.eu/images/stories/deliverables/ d4.1.5-final_hci_research_report-public.pdf

IX Raven, R. P. J. M., and Geels, F. W. 2010. Socio-cognitive evolution in niche development: Comparative analysis of biogas development in Denmark and the Netherlands (1973-2004). *Technovation* 30 (2): 87-99.

X Rip, A., and Kemp, R. 1998. Technological change. In *Human Choice and Climate Change,* ed. S. Rayner, E. L. Malone, 327-399. Columbus, OH: Battelle Press.

XI Rip, A., and te Kulve, H. 2008. Constructive Technology Assessment and Sociotechnical Scenarios. In *The Yearbook of Nanotechnology in Society, Volume I: Presenting Futures,* eds. E. Fisher, C. Selin, J. M. Wetmore, 49-70. Berlin etc: Springer.

XII Robert, L. (Jr.), Denis, A., and Hung, Y.-T. 2009. Individual Swift Trust and Knowledge-Based Trust in Face-to-Face and Virtual Team Members. *Journal of Management Information Systems* 26 (2): 241-279.

[XIII] Russell, S., and Williams, R. 2002. Social Shaping of Technology: Frameworks, Findings and Implications for Policy. In *Shaping Technology, Guiding Policy: Concepts, Spaces and Tools,* eds. K. H. Sørensen, R. Williams, 37-132. Cheltenham: Edward Elgar.

[XIV] Schot, J., and Rip, A. 1997. The Past and the Future of Constructive Technology Assessment. *Technological Forecasting and Social Change* 54 (2-3): 251-268.

[XV] SecureSCM (Secure Supply Chain Management). 2010.01. D7.2, *Cost and Benefit Analysis & Scenario Recommendations.* Available online: www.securescm.org/index.php?option=com_docman&task=doc_download&gid=12&&Itemid=24

[XVI] SHIELDS (Detecting known security vulnerabilities from within design and development tools). 2010.23.06. D5.3, *Final Evaluation Report*. Available online: http://shields-project.eu/files/docs/D5.3%20Final%20Evaluation%20Report.pdf

[XVII] Stewart, J., and Williams. R. 2005. The Wrong Trousers? Beyond the Design Fallacy: Social Learning and the User. In *User involvement in innovation processes*. Strategies and limitations from a socio-technical perspective, ed. H. Rohracher. Munich: Profil-Verlag. Available online: citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7713&rep=rep1&type=pdf

[XVIII] TAS3 (Trusted Architecture for Securely Shared Services). 2011.31.12. D9.2, *Pilot Evaluation Report*. Available online: http://homes.esat.kuleuven.ac.be/~decockd/tas3/final.deliverables/pm48/TAS3-D09p2-Pilot_Evaluation_Report.pdf

[XIX] Tushman, M. L., and Rosenkopf, L. 1992. Organizational Determinants of Technological Change: Toward a Sociology of Technological Evolution. In *Research in Organizational Behavior*, Vol. 14, eds. B. M. Staw, L. L. Cummings, 312-347. Greenwich: JAI Press.

[XX] UaESMC (Usable and Efficient Secure Multiparty Computation). 2011.31.07. D1.2, *Requirements specication based on the interviews.* Available online: http://ec.europa.eu/information_society/apps/projects/logos/1/284731/080/deliverables/001_D12.pdf

[XXI] UTRUSTit (Usable TRUST in the Internet of Things). 2012.30.04. D6.2, *Design Iteration I: Evaluation Report.* Available online: http://www.utrustit.eu/uploads/media/utrustit/uTRUSTit_D6.2-Evaluation_Report_final.pdf

[XXII] Van Dijk, J. A. G. M. 2010.30.04. Conceptual Framework. Study on the social impact of ICT. Eindrapport (EU-SMART PROJECT: CPP N 55A - SMART N 2007/0068). Study on the Social Impact of ICT (Topic Report 3). Brussel: Europese Comminissie, DG Informatiemaatschappij en Digitale Agenda.

[XXIII] Williams, R., and Pollock, N. 2012. Moving Beyond the Single Site Implementation Study: How (and Why) We Should Study the Biography of Packaged Enterprise Solutions. *Information Systems Research* 23 (1): 1-22

[XXIV] Wyatt, S., and Balmer, B. 2007. Home on the Range: What and Where is the Middle in Science and Technology Studies? Science, *Technology, & Human Values* 32 (6): 619-626.