Privacy and Identity Management in Europe for Life

Second thoughts on the WP 1.3 demonstrator

Editors:	Marit Hansen (ULD), Leif-Erik Holtz (ULD)
Reviewer:	Stuart Short (SAP) Peter Wolkerstorfer (CURE)
Identifier:	H1.3.7
Type:	Heartbeat
Class:	Public
Date:	October 31, 2010

Abstract

This heartbeat bases on and refines the general requirements for “Privacy for Life” (cf. H1.3.5) while applying the findings to the concept for the WP 1.3 “Privacy-Enhanced Backup and Synchronisation Demonstrator” (cf. H1.3.6). It takes the approach to add second thoughts to the conceptualisation and implementation phase of the demonstrator that can be more helpful to influence the design and to set the stage for the forthcoming work than the abstract requirements in previous heartbeats. In particular this heartbeat shows how socio-cultural requirements that have been identified and used already in PrimeLife’s predecessor project PRIME can be applied to the demonstrator and which of these requirements are less relevant for it. Moreover it focuses on delegation issues and sketches possible extensions or refinements that should be considered when developing the prototype. Finally it depicts further use cases related to the demonstrator.

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 Schleswig-Holstein	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.*

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	Marit Hansen (ULD), Leif-Erik Holtz (ULD)
1 Introduction	Marit Hansen (ULD), Leif-Erik Holtz (ULD)
2 Socio-cultural requirements for the demonstrator	Hans Buitelaar (TILT), Arnold Roosendaal (TILT)
3 Privacy-related requirements for delegation	Marit Hansen (ULD), Leif-Erik Holtz (ULD)
4 Further potential scenarios and use cases	Marit Hansen (ULD), Leif-Erik Holtz (ULD), Aleksandra Kuczerawy (K.U. Leuven), Karel Wouters (K.U. Leuven)
5 Conclusion and outlook	Marit Hansen (ULD), Leif-Erik Holtz (ULD)

Executive Summary

Workpackage WP 1.3 elaborates requirements for “Privacy for Life”, proposes solutions and illustrates them in a demonstrator dealing with “Privacy-Enhanced Backup and Synchronisation”. The concept of this demonstrator has already taken into account many of the requirements drafted in previous heartbeats. However, an interdisciplinary discussion on the concept and the implementation of the demonstrator among the partners is helpful because it enables an iterative process in the design and refinement of the current outline of the demonstrator.

The “Second Thoughts on the WP 1.3 Demonstrator” shows how socio-cultural requirements that have been identified and used already in PrimeLife’s predecessor project PRIME can be applied to the demonstrator and which of these requirements are less relevant for it. In particular the necessity of supporting the so-called “primary user”, i.e. the data subject holding the data items for which backup items will be created, in being and staying really in control over her data as well as the benefit of successful audience segregation are stressed. Besides, this heartbeat focuses on the issue of delegation. It describes possible extensions or refinements that should be taken into account when developing the prototype. To name only a few requirements: This comprises a clarification on the possible rights that are transferred or assigned to a delegate. In addition it should be distinguished whether the conditions for the delegate to act with an actual power of authority are met and he is expected to perform actions on behalf of the user or whether the delegate must not interfere because he does not possess the power of authority at a specific point in time. Moreover the question of logging the delegate’s actions or other ways for the primary user to trace back what the delegate did with respect to her data should be tackled in the demonstrator.

Finally further usage scenarios elicit specific requirements or design options that professional providers of a backup and synchronisation service should keep in mind. This section is not meant to deliver mandatory requirements that have to be fully implemented by the demonstrator, but it shows the possible embedding of the service and stresses the potential value of solutions that consider the interests of all parties involved.

Table of Contents

Chapter 1

Introduction

The objective of PrimeLife's Workpackage WP 1.3 is to elaborate requirements for "Privacy for Life" and present solutions in a demonstrator. Previous public heartbeats dealt with:

- the analysis od privacy and identity management throughout life (H1.3.3 [RSLB09]),
- requirements and concepts for identity management throughout life (H1.3.5 [StHR09]),
- conceptualising a privacy-enhanced backup and synchronisation demonstrator (H1.3.6 [DBPK10]).

Further work in the context of PrimeLife tackled building blocks for identity management throughout life [HaPS08] or focused on the topic of delegation [HRSZ10].

This document comments on heartbeat H1.3.6 that describes properties and concepts of the WP 1.3 privacy-enhanced backup and synchronisation demonstrator. It aims at refining the chosen concept with a focus on specific criteria for "Privacy for Life".

The privacy-enhanced backup and synchronisation demonstrator will enable a so-called primary user[1] to backup her data items at a storage provider. In case the primary user is in need of support of another person because she is temporarily not able (or not willing) to access her data, she can assign a delegate who may access her data on her behalf, possibly when predefined conditions are fulfilled. A delegate may also be appointed by a delegator that is not the primary user herself. Assigning a delegate is done by sending a delegation request to a delegation candidate that he can accept or decline on the basis of information on what partial identity initiated the delegation request, for what data, and under which conditions will the delegator be able to perform what operations on this data. The delegate candidate is informed that he can revoke delegated access

[1] According to H1.3.6, the primary user is the data subject owning/holding the data items for which backup items will be created. The notion of "owning the data items" is meant purely technical in the context of H1.3.6. Since the legal concept of "ownership of data" poses many questions with regard to privacy and data protection (not only) in the European framework, we focus on the notion of "holding the data items" and skip further elaboration of potential frictions concerning "owned" data.
For better understanding, we use the female form for the primary user, but the male form when talking about a delegate.

rights any time in the future if he accepts the request. The delegation can be restricted to particular areas of life or particular partial identities of the primary user.

The sketched concepts work on the basis of encrypted data and credentials for proving one’s authorisation. With this concept the demonstrator directly addresses several issues of “Privacy for Life”: It provides a possibility for users to store their data safely over a long period of time, it distinguishes between various areas of life by separating the data of different partial identities, and it offers delegation of access rights which may be necessary if the user cannot manage her (backup) data on her own.

This heartbeat contributes to the development of the demonstrator by choosing relevant issues that should or could lead to refining its concept. The text is organised as follows: First, chapter 2 makes use of the knowledge base of PrimeLife’s predecessor project “PRIME – Privacy and Identity Management for Europe” by applying the socio-cultural requirements developed back then to scenarios basing on the WP 1.3 demonstrator. Chapter 3 continues with addressing the issue of delegation which leads to further requirements to realise in the concept or even in the implementation of the demonstrator. Additional aspects of interesting scenarios or use cases are mentioned in chapter 4. These extend the current scope of the backup and synchronisation demonstrator and thereby show possible evolvements. Finally chapter 5 concludes the text with a short summary and an outlook.

Chapter 2

Socio-cultural requirements for the demonstrator

This chapter deals with the socio-cultural requirements for the demonstrator and is based on the socio-cultural requirements derived from the project PRIME – Privacy and Identity Management for Europe.

In PrimeLife's predecessor, the PRIME project, a list of socio-cultural requirements was established. These requirements relate to privacy and identity management. A number of them, however, can also be relevant for this demonstrator. First, here the entire list of requirements will be repeated and, then, the relevant ones will be indicated. These requirements should contribute to a refinement of the requirements to the demonstrator.

2.1 Overview about the socio-cultural requirements from PRIME

In the "PRIME Requirements V3" [Schu08] a distinction was made in three key aspects, the "umbrella terms", which are relevant from a socio-cultural perspective. These umbrella terms are

- audience segregation,
- control, and
- adoption.

Control is constituted by ten requirements, namely: "comprehension", "consciousness", "consent", "choice", "confinement", "consistency", "context", "inspection", "chain control", and "ex-post user control". Adoption is constituted by six requirements: "social settings flexibility", "minimise skill level", "accountability", "trust in transaction partners", "trust in communication infrastructure", and "affordability". Requirements can influence each other and sometimes they overlap.

2.1.1 Audience segregation

Audience segregation is very relevant in the context of the demonstrator. The primary user should be able to have different partial identities to play different roles and portray the self to others in a way she chooses. With regard to the demonstrator, this means that the contents of the backup have to be divided in categories belonging to the different audiences the individual interacts with. Once, the backup system is needed to provide a person (second party) with information or contents belonging to an individual, access to the backup needs to be restricted to the parts that have to be disclosed to the aforementioned second party instead of permitting it to access all the content in the backup and selecting the relevant parts themselves. The issue of audience segregation should be taken care of in the demonstrator by letting the primary user provide others with access rights, either directly or via delegation. These access rights should be connected to specific parts of the content. Besides, the content itself needs to be encrypted, so that visibility for second parties does not directly imply a "real" disclosure of the content. In this way the issue of audience segregation can be solved in the demonstrator.

There is, however, a specific point of attention, which is related to indicating or defining the audience and having control over this. A distinction can be made between the intended audience and the actual audience. The intended audience is the audience which was meant to have access to content in the backup system. So, this is the second party to whom access rights were granted or delegated. The actual audience is the audience that in practice has access to the content. This can be different from the intended audience when more or other people have access, for instance when the access rights are distributed to others, or when the originally intended audience has changed in composition. That can, for instance, be the case when a colleague has also become a family member in the meantime and, therewith, has access to work-related as well as family-related documents. Here, the segregated audiences come together and contexts collapse. The consequences of this will depend on the way the colleague deals with this.

Apart from this, it is questionable whether this problem can be solved in the demonstrator anyway. Changes over time in people's contexts are difficult to grasp in a technical solution. Nevertheless, a proper delegation system may solve the issue. When a third party is responsible for delegating the access rights when necessary, the distribution of access rights can take place at the moment when it is necessary and does not have to take place (possibly long) beforehand. This implies that the intended audience can be reviewed at the moment of granting the access rights.

2.1.2 Control

Control means that the user has control over what happens with her personal data. This is relevant not only for the primary user, but also for the delegates as far as their personal data are concerned.

For the primary user[2], this comprises in particular the data items for which backup items will be created, the backup items, usage data that is created when using the backup system, information on requests to delegation candidates and delegates and the communication regarding the status of the primary user that may be communicated to delegates. For delegates (and delegate candidates), privacy-relevant data may be usage data as well as requests from the primary users or credential issuers. So not only the data items themselves, but also information on a delegation (candidate)

[2] In addition to the "primary user" and "delegates", H1.3.6 defines the actors "backuper", "restorer" and "deleter". Here we assume that they should be understood as roles taken by the primary user or a delegate rather than being actors themselves. If they were actors, at least their usage data may be privacy-relevant so that all control requirements would have to be considered for them, too.

relationship between a primary user and a delegation (candidate) as well as usage data have to be taken into account when dealing with the control principle.

In the light of the demonstrator the control principle means among others that the primary user decides what is stored in the backup, who has access, and can check along the way and afterwards whether things went as intended. The aspect of control is constituted by ten requirements. Each of them will be discussed here briefly.

2.1.2.1 Comprehension

Comprehension means that the primary user as well as delegates should understand how their personal data are processed by the service provider. For the demonstrator this means that the primary user and the delegates have to understand what happens to their personal data.

Basically, the primary user will often have the role of service provider herself when using the backup tool, so then it is necessary that the primary user understands what exactly happens when she is doing something with her data. Thus, the system and its functionalities itself need to be comprehensible. Next to that, there may occur situations where others process the data, for instance, when the data are stored on another machine than the primary user’s own computer. Then, the owner of the other machine can probably be qualified as a service provider. At least there is the service of hosting or providing backup space.

It has to be clear to the primary user whether the tool is running on the primary user’s computer after installation or whether the service is or can also be provided by a third party at a distance, who then can be qualified as a service provider.

2.1.2.2 Consciousness

Consciousness is described as: “the user should be aware of the essential events, processes, stakeholders and attributes of the collection and use of personal data.” Consciousness is a necessary condition for the exercise of data subject rights such as consent, right of access and right to object. When a primary user uses the backup system, she has to be aware of the processes involved in the backup and who is involved in the processing of the data. Similarly the delegates have to be aware of privacy-relevant aspects of the backup system – both in the relation with the storage provider and with the primary user.

In the demonstrator, the data subject takes the role of a user and creates the backup. This implies that there is consent and that the data subject is aware of the data being processed. The exact process, however, also needs to be transparent and comprehensible. Only then will the primary user (or a delegate) be in a position to be aware of (possible) second or third parties that may have access to the data or process the data otherwise. Exact technical knowledge may not be necessary, but some knowledge about the exchange of data and access to data is essential.

2.1.2.3 Consent

As indicated above, the requirement of consent is fulfilled in the demonstrator since the data subject is the primary user of the backup system and initially processes the data herself. Processing by others is based on delegation and access rights, meaning that the primary user also has consented for this (further) processing.

Further the delegates have consented to be delegates which means that they have to know what is expected from them and how the primary users or others may control their behaviour. Note that the delegation candidates have not given consent to be delegates.

2.1.2.4 Choice

Choice means that the primary user should have choices regarding all data collection activities concerning her personal data. Taking into account that the idea of the demonstrator is to give the user all control over the processing of her data, this requirement is less relevant. As long as the primary user is not forced by the system to process more data than strictly necessary for the purpose of the backup system, there is no need for an alternative system to provide the primary user with choice concerning the system used for backing up data. The same is valid for delegates.

2.1.2.5 Confinement

Confinement is in fact a very broad term. It covers the well-known principles of purpose specification and purpose binding – or better even: use limitation. This entails that the primary user should be able to set limits on who may access her personal data and for what purpose. Moreover confinement relates to security safeguards because the user should be able to set limits on who may access personal data. These requirements obviously are also legal rights and duties, but they may be hard to enforce in practice. The PRIME vision is that mechanisms to enforce these legal requirements should be embedded in techniques and applications.

The demonstrator ought to take care of these requirements properly by calling for inter alia minimisation of linkability of personal data (risk of "function creep") and also minimisation of multipurpose or context-spanning use of personal data. Storage providers are thus prevented from using the personal data of the primary user for different purposes (e.g., accounting purposes). Likewise attention needs to be given to security requirements such as planning for emergency situations. Data controllers also have to foresee beforehand procedures for erasure of personal identifiers after their usage period. As such, the demonstrator will fulfil the following targets of the PRIME requirement of confinement by providing ways to express preferences/policies with respect to:

- the purpose of use of the personal data,
- who may have access to the (personal) data,
- where they may be stored,
- until when they may be stored.

It also should provide the necessary security safeguards to keep personal information within its determined boundaries.

This is not only necessary for the data items and backup items, but also for usage data of primary user and delegates and for requests between primary user, delegates and credential issuers.

2.1.2.6 Consistency

The requirement of consistency is very much tied up with the so-called digital identity of the primary user. Contextual dependency plays an important role here as well. The context dependence necessitates that the primary user is informed about the use that is to be made of the data she provides via the application, because each application potentially gives rise to new and unknown uses and ensuing identities. These uses and identities still lie in the future at the moment the primary user relinquishes her personal data to the application. In other words, there is a time lag between the principal moment at which the primary user is able to exert control and the moment the digital identity comes into existence. The primary user must be given insight into the future uses of the personal data she provides. This glimpse into the future must be constructed with as much consistency as possible. The principle of consistency is therefore related very much to the requirements of control and transparency.

The demonstrator ought to take much note of this requirement. It should elaborate the transparency requirement from the scope of revocability and irrevocability. It should prescribe that for all parties involved it should be clear at all times what the potential impact can be of decisions and under which circumstances they can be revocable or irrevocable. Data controllers have to inform primary users of the ir-/revocability of their decisions. The primary user must be aware that she can always delete any item of her personal data in all locations and in all existing instances. The primary user should also be able to refuse access rights delegated by a delegator at any point in time.

2.1.2.7 Context

The requirement of context is linked to the requirement of audience segregation and choice. The caveats noted about the differences between “intended” and “actual” audience can be brought to bear here as well. However, contexts bring into play new elements because context tries to take account of situational factors affecting individual perceptions and desires for privacy. It also takes into consideration the kind of information in question, in terms of its perceived sensitivity. For young people the definition of sensitive information is frequently very different from what is specified in data protection and privacy laws. Not only age differences play a role here but also broader socio-cultural variables. Situational or physical contexts may affect the primary user’s privacy preferences to a large degree.

The demonstrator should seek solutions for separating the personal data of the primary user according to her different areas of life because these areas belong to different contexts. All the same the proper delegation of sufficient access rights by secure access control mechanism needs to be implemented. The primary user usually should be in full control of the selection of these access rights; delegators others than the primary users should be the exception (e.g., in emergency cases or on a predefined basis), and even their actions should be comprehensible by the primary user. Of course, the confidentiality of the personal data can be guaranteed by data encryption before sending it to the storage controller. Important measure in this respect will be the utilisation of the anonymisation service which separates the different areas of the primary user’s life. Context separation can also be ensured by anonymous credentials unique for every backup.

2.1.2.8 Inspection

Inspection relates to the control requirement because users must be able to check whether their actions have the desired effects. It is as such a key requirement to establish transparency. Obviously, data subjects have legal rights, such as to be informed about the processing of personal data, the identity of the controller and the purpose of the processing. But these rights need to be implemented to make sense and be effective. As such inspection is a means of ex-post user control.

The demonstrator ought to take care of this requirement by adopting all this type of information in the End User Licence Requirement which the primary user will have to accept before using the service. In start-up windows, interactive help information during the use of the application, and a wizard, which provides the user helpful information related to the action at hand, much attention can be given to this requirement. Information can also be provided about the risks of linkage and the granting of access rights to delegates. A search functionality can also be included in order to permit the user to visualise which kind of data is stored in which backup.

Note that primary users often wish or even need to check whether the actions of delegates performed on their behalf don't violate what has been agreed upon. And also delegates may desire some inspection possibility as far as their personal data are concerned.

2.1.2.9 Chain control

The primary user and delegates should be able to inspect data collection and use throughout the service chain. Following from the requirement of inspection, users (i.e. primary users and delegates) should be able not only to inspect the actions of a data collector, but also the actions of the multiple service providers which are present in the interaction chain. As such, chain control is a specification of the inspection requirement.

In general, chain control means among others: On the user's request, the application should provide information for each party involved about:

- When personal data has been disclosed?
- To what parties this data has been provided?
- Under what conditions the data has been provided?
- Who had access to the data?
- For what purpose they had access to the data?
- Why and how data is used?

The application should also allow for informing the user later on about a new link in the chain (for example when a new organisational structure of a business where the user is employed is introduced) and if so, make it possible to change or withdraw consent.

The demonstrator should pay much attention to fulfilling these requirements. This is of special importance in the case of third parties becoming delegates of a particular backup. Every delegate candidate is then informed who initiated a delegation request for what data and under which conditions the delegator will be able to perform what operations in this data. The delegate candidate should be informed that he can refuse (revoke) delegated access rights anytime in the future if he accepts it. Selection of proper access rights should be under full control of the primary user.

Special attention should be paid to the user interface which informs the primary user that the storage provider may cancel the contract if the primary user does not follow the requirements of the contract, e.g., if the primary user refuses the contractually agreed payment). This should only be possible within an accepted and previously communicated legal setting. Perhaps this could result in disclosing the personal information of the primary user to enable the storage provider to take legal action.

2.1.2.10 Ex-post user control

This requirement is closely linked to the requirement of inspection and, it hardly needs saying, user control. Ex-post user control is control after the fact. Therefore it builds on the legal requirement of the right to rectify, erase or block the data (Article 12 of the Data Protection Directive 95/46/EC). From a social perspective this is an important requirement because personal data are increasingly used as the basis for making decisions concerning an individual. If the data are incorrect, outdated or not relevant, the decision can turn out to be incorrect, and hence, users must have the possibility to correct or object. In addition, ex-post user control is an indicator of how people perceive the service and is therefore related to comprehension and consciousness.

In the context of minimising irrevocable consequences the demonstrator should implement a function which allows for deletion of any backup item and its derivates in whichever backup of the primary user. Solutions should also be provided for backup and removal of a single item taking into account an encryption schema, anonymity, unlinkability and unobservability during transmission. The demonstrator will then provide sufficient opportunity for removal and deletion of data by the primary user. Special attention should be given to also providing a mechanism for rectification.

2.1.3 Adoption

The demonstrator should be designed to maximise adoption by its target audience. Obviously, a tool which is not used is useless. However, not only the use as such is of importance, but also the use by a (large) group. Only when a bigger audience is reached will the tool contribute to improvement of identity management capabilities of individuals and at the same time prevent the risk of a digital divide between users who can manage their identity and personal data and those who cannot.

2.1.3.1 Social settings flexibility

This issue is probably not or only less relevant here. It deals with perceptions of public and private, but in the prototype all data are primarily considered as private data.

2.1.3.2 Minimise skill level

This requirement means that the user should be able to use the tool with a minimal amount of training. So, the purpose of the tool has to be clear and the interface has to be user-friendly. This user-friendliness should count for a general public, so not only people with technical skills, but also ordinary users. The demonstrator should strive for a clear and comprehensible user interface.

2.1.3.3 Accountability

This issue is probably not or only less relevant here, because the tool’s primary purpose is not to act anonymously. However, the access to the system based on pseudonyms, either by the primary user or by a delegate, has to be accountable. This is an access control issue which should be taken care of by means of credentials.

2.1.3.4 Trust in transaction partners

This issue is probably not or only less relevant here – the demonstrator doesn’t focus on transactions, but on access to data. Surely trust in delegates is essential for the privacy-enhanced backup and synchronisation demonstrator, but it mainly has to be tackled outside the IT system.

2.1.3.5 Trust in the communication infrastructure

The user has to be able to assess the trustworthiness of the communication infrastructure. So, how secure is the backup, can others access it or not, how do things work when someone else must access the data? Requirement therefore is that this is dealt with properly by means of an access control system. Access control and authorisation should also be dealt with in relation to security. End-user trust must be provided by usability, also, because usability can contribute to transparency of the system and therewith increase trust. If a system is too incomprehensible (not user-friendly), trust is difficult to establish.

2.1.3.6 Affordability

The tool should not be too costly for users to obtain and use. If it is a software tool that can be distributed fairly easily, this will be no problem. However, it should also be easy to install in order to prevent the tool from being costly in terms of time spent.

2.2 Interim results

The requirements depicted above should be conceptualised in the demonstrator design in a corresponding way and implemented as far as possible.

Chapter 3

Privacy-related requirements for delegation

This chapter focuses on privacy-related requirements for delegation in the privacy-enhanced backup and synchronisation demonstrator. After giving definitions from [HRSZ10], the setting of delegation in the WP 1.3 demonstrator is explained (see section 3.1). On this basis, several requirements on how to tackle delegation in the demonstrator are identified (see section 3.2), in particular on limiting the delegate's access to the necessary extent, on controlling the delegate's actions and in the area of delegation based on legal provisions.

3.1 The setting of delegation in the demonstrator

In this heartbeat we address privacy aspects of delegation as a means to support individuals in stages of life when they cannot act on their own or are not willing to act on their own regarding some aspects of their privacy although they might be capable to do it.

To clarify our understanding of delegation, we quote the following definitions from [HRSZ10] that are in line with the legal terminology:

> ***Delegation:*** *Delegation is a process whereby a* **delegate** *(also called "proxy", "mandatory" or "agent") is authorized to act on behalf of a person concerned via a mandate of authority (or for short: mandate).*
>
> *The* ***mandate of authority*** *usually defines in particular*
>
> *(1) the scope of authority for the actions of a delegate on behalf of a person concerned and*
>
> *(2) when and under which conditions the delegate gets the power of authority to act on behalf of the person concerned.*
>
> *The delegate shall only act on behalf of the person concerned if the delegate has the actual power of authority and if his action lies within the scope of authority. The simple acting of the delegate with the existence of a mandate while not having the power of authority would not be sufficient. The difference between mandate and power of authority becomes clear in the following example: In working life the schedule of responsibilities*

> *may determine that person A should take over the work of colleague B if the latter is absent. The issuance of the mandate of authority to A is expressed by the schedule of responsibilities, but the A's actual power of authority only comes into existence if B is absent. Otherwise A must not act on behalf of B.*
>
> *The mandate of authority is issued by the* **delegator** *(also called "mandator"). This may be the person concerned herself, but there are also cases where other entities explicitly decide on the delegation (e.g., in the case of incapacitation of a person the guardianship court rules on delegation) or where the delegation is foreseen in law (e.g., when parents are the default delegates of their young children). The mandate of authority is usually assigned for a specific period of time. Similar to the process of issuing a mandate, changing or revoking the mandate can be done by the delegator, i.e., by the person concerned herself or by other entities. The conditions and processes to issue, change, or revoke a mandate can be defined by the underlying contract or law.*
>
> *Note that not always the delegate is aware of the mandate of authority or of the fact that he actually has the power of authority. So the delegator should implement an appropriate way of informing the delegate (and the person concerned if she is not the delegator herself) about the mandate and the power of authority.*
>
> *For supervising purposes of the delegation and related actions by the parties involved, one or more impartial* **delegation supervisors** *may be appointed by one or more of the actors. In particular the person concerned may have the need to check whether the delegate really acts as agreed upon.*

The concept of the WP 1.3 demonstrator that was sketched in the PrimeLife heartbeat H1.3.6 takes a slightly deviating approach [DBPK10]:

> *"**Delegate:** is an entity, which receives particular rights on the backup from a delegator.*
>
> ***Delegator:** is an entity, which has the privilege to delegate rights to delegates concerning a particular backup. In most applications of this demonstrator, the primary user acts as the delegator.*
>
> ***Delegate candidate:** is an entity, which was selected by delegator to act like delegate but does not possess particular rights yet.*
>
> ***Delegation request:** is a request sent to the delegate candidate asking him whether he accepts particular rights from the delegator.*
>
> ***Credential issuer:** is an entity, which issues a credential verifying a certain status of the primary user. This status can for example be: "primary user is ill", "primary user is hospitalized", "primary user is dead" or others. A credential issuer must be authorised by a corresponding authority (e.g., governmental) for issuing a certain type of credentials."*

Similar to the definitions in [HRSZ10], the delegator (which may be the primary user herself) has the privilege to delegate rights to delegates in the H1.3.6 setting. As a mechanism, a delegation request is sent to a delegation candidate who can accept or refuse being a delegate concerning particular rights. From [DBPK10] it is not fully clear what "particular rights" the demonstrator will support: Presumably it should only mean "reading access" to predefined backup items (under a defined partial identity of the primary user, possibly only the newest last version and possibly for a limited period in time). But it could also mean that the delegate may back up items from the primary user (e.g., if the delegate acts on behalf of the primary user in a transaction, the relevant data could be put into the backup), that the delegate may restore (or copy) the backup on another computer (which may be necessary if the delegate should act on behalf of the user), that the delegate may conclude a new contract with another storage provider, or that the delegate may cancel an existing contract with a storage provider.

3.2 Requirements for delegation

On the basis of the outlined definitions and concepts in the previous section, this section sketches various requirements for the integration of delegation into the concept and possibly implementation of the WP 1.3 demonstrator.

3.2.1 Limiting the delegate's access to the necessary extent

As already discussed in chapter 2, the delegate's access should be limited to what is necessary. This comprises the limitation to one or few partial identities of the primary user as well as a limitation of the possibility to exercise the access rights to a certain period of time.

The delegator should be supported in limiting the delegate's access rights by the user interface of the backup system. By default, only access to the newest backup as well as to data belonging to one partial identity of the primary user should be offered. The system should inform the delegator that the access could be even further restricted, namely to specific backup items. It should explicitly ask for the period of time that the delegate should be assigned the according access rights. By default it should not be unlimited, but extensions should be possible if necessary (e.g., in the case of a hospital stay of the primary user which turns out to be longer than expected).

The backup system should support the delegator in the following steps:

- How to generate delegation requests to delegate candidates?
- How to deal with their (positive/negative/missing) answers to those requests?
- How to revoke the status of being a delegate?
- How to limit the access rights of the delegate?
- How to communicate possible conditions to being a delegate or conditions to having the actual "power of authority"?
- How to communicate to the delegate that he is assigned the actual "power of authority"?

The question of the actual "power of authority" that a delegate should have if he acts on behalf of the primary user is tackled in [DBPK10] by issuance of a "credential verifying a certain status of the primary user". For visualising the functionality of the demonstrator, this construction may be sufficient. Still from a data minimising perspective it should be clarified which information is necessary in each case to be transferred and who sees that information (the credential issuer? the delegate? others?). In particular it is very often not necessary, but even privacy-invasive to give information on the medical status of the primary user.[3] In several cases it could be sufficient to communicate "delegate receives the power of authority from <beginning> to <end>". For delegates it is very relevant to know whether the power of authority is only given for a very short time so that he only has to handle urgent requests and could delay the non-urgent requests, or whether the power of authority should last for a longer time. Even in case the exact timeframe of the power of authority cannot be given in the beginning, this fact as well as a minimal or estimated duration for the power of authority should be communicated to the delegate. This could also mean

[3] Note that contrary to the impression imposed by the following quotation, pregnancy as such usually does not have an impact on the ability of the primary user to manage her privacy: "State of life: temporary or permanent state of the data subject's life, which can be certified by a corresponding credential issuer and which might have impact on the ability of the data subject to manage his data (e.g., illness, hospitalization, death, pregnancy, imprisonment and others)." [DBPK10]

that the delegate gets multiple messages for prolonging the power of authority or refining the information given in a message before.

3.2.2 Controlling the delegate’s actions

The primary user should always be in full control over the access possibilities of the delegate and should also be able to reconstruct the actions the delegate has performed on behalf of the primary user. A precondition for this is the information of the primary user of the assignment of delegates (or delegate candidates) and their potential or actual rights concerning the backup. This is important to maintain an overview on the delegation at all times, but it is even more necessary in case the delegator who initiated the delegation is not the same person as the primary user.

It is mandatory that the delegates do not use the same credentials as the primary users to perform their actions because otherwise these actions would not (or not easily) be distinguishable from actions from the primary user. Concerning delegation to organisations where multiple members (e.g., employees) could act as delegate, each individual person should use their own credentials. There should be more than one credential per delegate if they are assigned access rights for different backups (different users or different partial identities).

Actions taken by the delegate concerning the data of the primary user must be traceable by her so that she can check later on any action performed with respect to her data. If she cannot conduct the supervision herself, she may appoint one or more impartial delegation supervisors to look after her interests. For the demonstrator, this means that it should log actions performed by delegates for a predefined time and give access to these logs by the primary user. This has to be known both by the primary user and the delegate. The demonstrator could also foresee the possibility of delegation supervisors that cannot access the data of the primary user, but can access the logfile on the actions of the delegate. Delegation supervisors are delegates, too, but only in the function of supervising other delegate’s behaviour. They need own credentials to prove that they have specific rights. In case their actions (i.e., accessing the logfile) should be supervised, too, there would be the need for another logfile. Surely it does not make sense to implement a fully recursive (and thereby infinite) mechanism of logging and supervision. Moreover, there should not arise further risks for the privacy of the primary user – or the privacy of the delegate – by maintaining comprehensive logfiles for a long time. Here a good balance has to be found. There is no need for the demonstrator design to fully resolve this issue, but still it should foresee possibilities to log actions of the delegate and provide access to the corresponding logfile by the primary user.

In case the delegate should be allowed to assign further delegates with the same or derived access rights to the primary user’s backup, this has to be communicated to the primary user. This sub-delegation needs to be traceable later on, too. Similarly the delegate has to notify the primary user (as well as the delegator) if his credentials get lost or stolen or if he has the suspicion that somebody misuses his credentials. In case the delegate cannot perform the actions the primary user (or the delegator) expects, e.g., because the delegate’s stage of life does not allow it, this fact also has to be communicated to the primary user (and the delegator). It is not necessary that the demonstrator implements such kinds of notification, but the concept should mention the necessity of such functionality.

The primary user should be able to define the scope of authority of the delegate: Under which conditions should the delegate access which data? In addition, there may be specific preferences for post-mortal period that the primary user would like to communicate to her heirs or some delegates. For the purpose of the demonstrator the development of technology-supported mechanism to express conditions or preferences might be too ambitious.

3.2.3 Delegation based on legal provisions

The concept of the demonstrator in PrimeLife heartbeat H1.3.6 does not elaborate on different causes and procedures how the delegator may assign delegates. However, possible assignments of delegates have been depicted in an HCI prototype within the PrimeLife project [GWW+10]. The presentation of the prototype in that deliverable showed that it is not easy to design a clear and understandable user interface for assigning delegates by the delegator, and the desired functionality has not been fully spelt out, yet. In the following, a few issues related to different causes for delegation are described.

The instrument of legal representation is common in civil law where the powers of the delegate and the legal effectiveness of the delegation are predefined as well as the bounds of delegation. Many of the scenarios depicted in PrimeLife heartbeat H1.3.6 contain delegation aspects based on the will of the individual. However, the delegation may also be based on legal provisions, e.g., if the delegate is the legal representative of the primary user according to law or a court decision. This is especially relevant if backup items contain not only private diary entries, but something relevant to official transactions (e.g., governmental certificates or insurance documents).

Law defines generic roles (and associated conditions to check that a person is playing that role lawfully) in addition to family relationship in cases where the primary user, over majority age, is unable to manage her own data (e.g., mental disability). Several types of roles and levels of delegation might be defined, with more or less control over the person’s data, in accordance with their role in assisting the primary user in her everyday life.

3.2.3.1 Delegation by a legal representative based on court order

The first question is how to prove that a person is a legal representative of a primary user. Today, the proof (e.g., a court order) would have to be shown to the storage provider. In the setting of the demonstrator this other party may rather be the credential issuer. However, a prerequisite would be to know that the primary user has used the backup service of specific storage providers.

Current legal concepts usually don’t distinguish between different partial identities – instead, the task of a legal representative in the sense of the civil law is to represent a person in all contexts. This would mean to give access to all backup items of the primary user, irrespective of the chosen partial identity. Of course the primary user could plan ahead for possible legal representatives, e.g., by only informing them about specific partial identities or individually encrypting data she does not want to disclose to her legal representative.

3.2.3.2 Access to backup items from deceased persons

In situations where a person has died, the instrument of law of succession applies [StHR09]. Therefore the legal basis for deceased people is as follows: The European Data Protection Directive 95/46/EC assigns the right of privacy and data protection in Article 1 to “natural persons”. Deceased people are no longer regarded as data subjects. Nevertheless, protection against an unregulated processing of data concerning deceased individuals in some European legal frameworks is provided by means of a “post-mortal personality right”[4].

The primary user could determine beforehand how her backup items should be handled after her death (containing order for further storage, deletion blocking or delegation). In this approach, the

[4] This applies at least for Germany, see the so-called “Mephisto decision” of the German Supreme Court, BVerGE 30, 173.

primary user would give orders similar to a testament. This has the advantage that the way of handling the data would be defined even beyond death. However, in the applicable civil law (e.g., in Germany, section 1922 BGB) this might conflict with the role of the "universal successor" that reserves all rights and all duties from the deceased individual (or simply the inheritors). This typically includes the right to decide what happens to the individual's rights – and her goods. Although this usually does not include the right to determine about the individual's personal data, the access to some backup items may be necessary to know about relevant financial assets or to access digital goods stored in the backup that now belong to the heirs.

Another question would be which influence the death of the primary user could have on the delegation. The mandate – as long as it is not limited to the primary user's lifetime – is still valid when she deceases. The universal successor has to revoke this delegation if he does not want the delegate to have access rights to (certain) backup items of the individual. Therefore it is doubtful, whether the backup system has to inform the delegates about the primary user's death or whether the backup system just would have the obligation to inform the universal successor about existing mandates. Following the principle of data minimisation, the second approach seems to be preferable. The universal successor has to legitimate to the backup system, afterwards the backup system has a contract with the universal successor (including all rights and all duties).

It is questionable whether the credentials of the primary user should directly be transferred to the inheritors in case of her death. For example a person from a group of inheritors should be prevented from accessing the data first, copying them and then deleting all the data so that the others don't have access to this information anymore. On the other hand, there may be personal files that are only meant to be read by one specific person within the group of inheritors. In any case inheritors should not work with the original credentials of the primary user, but be issued individual credentials. The possible conflicts (that are usually resolved in different ways according to national law) should not be dealt with in this version of the demonstrator.

3.2.3.3 Using the backup system for data from minors

Parents could manage a backup of official information concerning their children. Initially, the delegation works from the parents to the child, i.e. the child can have access to the data, but it is entirely managed by the parents until an age defined by law. The topic of delegation for children and teenagers has also been depicted before [StHR09][HRSZ10]. It includes the unusual feature that the delegate does not only act on behalf of the individual, but the delegate also has to decide, which access rights the child or teenager will get and when. In other words, in this scenario the delegate decides about the individual's access rights and not vice versa. At some point, the parents should decide to reverse the delegation: the child then gains control and the parents receive the delegated role. Then, this delegation should not be revocable by the child until the age of majority. In any case, at majority, the grown-up gets full control over the data without the necessity of involving the parents as delegates any more. The young adult also may decide to remove all the data from that storage provider and choose other services.

The scenario is different from the others described before because the law already defines that parents are legal guardians for their children. Insofar they can and should act as delegates for their children. The parents take over the role of a delegate (or rather two delegates) and in addition are in the role of the delegator (again: possibly two delegators) while their children are individual primary users.

Since this would reverse some functionality in the demonstrator, it could be mimicked in a way so that the parents first decide on which data to backup where and give each child the reading access rights as a delegate (although in principle it is a primary user). It should be negotiated whether the access of parents or kids are logged and if so, who gets access to these logfiles. Usually there is no real need for logging the activities (at least not in a trusted relationship), but this may not hold for all occasions.

Chapter 4

Further potential scenarios and use cases

This chapter deals with further potential scenarios and use cases that may extend the current scope of the privacy-enhanced backup and synchronisation demonstrator. First it is described how incidents could be handled by such a tool and its providers (see section 4.1). Then two examples of possible changes in the technical field are briefly outlined (see section 4.2). Finally, two more usage scenarios show potential extensions of the demonstrator (see section 4.3).

The developers of the WP 1.3 demonstrator should consider how the scenarios in this chapter may influence the design of the privacy-enhanced backup and synchronisation demonstrator. Most technical relevance has probably the possibility to migrate the used cryptographic functionality to other schemes (see section 4.2.1).

4.1 Handling of incidents

There could be a variety of incidents that would have to be tackled in case of occurrence. This section picks two relevant areas, namely the violation of the contracts between entities involved (see subsection 4.1.1) as well as the issue of search and seizure (see subsection 4.1.2).

4.1.1 Violation of the contracts between entities involved

The relationship between the primary user and the storage provider is determined by a contract. This contract has to contain information about the rights and duties of the respective parties. In particular the storage provider usually gives information on the planned or guaranteed availability of its service. In addition, a potential payment by the user for the service may be laid down in the contract. In case of violation of the contract by one party, the other party usually can cancel the contract. Here it is important to think about the consequences regarding the data that is being stored and the expectation of the primary user or potential delegates that the backup items are accessible.

When drafting or entering such a contract, it should be clear from the beginning:

- How can it be ensured that the primary user will maintain the control of personal data stored at the storage provider if the contractual relationship between the primary user and the storage provider is terminated? How long will the data be kept? And as soon as the data are deleted: Will the data be safely erased? If the data are still there: Will access of the primary user or a delegate be denied?
- In case of a paid backup and synchronisation service: What processes are established if the primary user is late with the payment or stops to pay for the service? For instance, if a regular payment is part of the contract, but the primary user is in hospital in need of the delegation functionality, but at least temporarily without the possibility to initiate the payment, how could this be handled? Clearly the primary user then should be informed about the missing payment, but should also assigned delegates be informed? Under which conditions should the storage provider reveal the name and address of a pseudonymous primary user to collect her debt? And what does this mean for the accessibility of the data – should the storage provider have the possibility to prevent any access of primary users and delegates in case of lacking payment? This may have critical effects.
- In case of bankrupt, mergers or corporations or sales of corporations on the storage provider's side: How can it be guaranteed that the level of protection originally ensured to the primary user will remain at least equivalent?

Also, a change of policies (privacy policies as well as general terms and conditions) on the storage provider's side may be a violation of the contract, but there may be changes that are in line with the contract, or there may be legally demanded changes that leave the storage provider with no option but to adapt the contract. In all these cases it would be necessary to inform the primary user and also delegates if the changes may affect them about the changes. Usually the persons involved have to affirm their consent.

In addition to the contract between the primary user and the storage provider there may be contracts between the primary user and the delegator (if they are not the same) or between the delegator and the delegate. Further the potential involvement of a delegation supervisor could be based on a contractual relationship. In all of these cases there may be questions of payment or liability issues if an entity does not act according to the predefined rules. How to handle these possible incidents should be clarified in advance to prevent any unpleasant surprise in the future.

In general, breaches of confidentiality, integrity or availability guarantees concerning the backup items or credentials should not happen, but if they occur, the other parties involved should be informed about the incident and possible precautions they can take to minimise undesired consequences. This can happen on the storage provider's side, on the primary user's side or on a delegate's side. There also may be liability issues, and compensation rules may be foreseen in the contract. Otherwise this may justify a legal claim for damages.

4.1.2 Effects of search and seizure

However, there is a special case which may have to be treated differently: search and seizure. In case police or law enforcement suspect that a crime has been committed, they have according to many civil law and common law legal systems the right to do a search of a person's property and confiscate any evidence that is potentially relevant to the crime. Regarding the backup and synchronisation system this may in principle happen on the side of all entities involved, i.e., the storage provider, the primary user, the delegator, the delegate, the credential issuer.

Search and seizure can mean that only a copy of the data from the IT systems are taken, but they are still functioning, or it can mean that the IT systems are taken away, often for some days or several months. In the latter case there is probably at least a downtime of some time until the functionality of the IT systems involved can be restored. The availability of the data and the functionality of the systems can be reduced even more if restoring the data is not possible.

Possible consequences can be that the service does not work or that parties such as the delegate cannot fulfil their tasks any more in case their credentials are gone. The primary user whose backup items are at stake is not necessarily the suspect in this scenario, but still may be influenced by a search and seizure procedure.

Depending on the legal scheme and the exact wording of a court order or other documents that have to be shown in a search and seizure procedure, it may be allowed or not allowed to immediately inform other parties about this incident. All parties involved should at least document what is happening when, so that later on (e.g., when a suspect has been cleared) the incident and possible consequences can be reconstructed. Usually the authority in charge has to inform the suspected individuals at least afterwards about the search and seizure procedure, even if they didn't notice it and no charges are pressed.

4.2 Handling of technical changes

Progress in technology provides new opportunities, but also poses new challenges. This section exemplifies that by the possibility of migrating the cryptographic functions (see subsection 4.2.1) as well as the deployment of cloud computing technology (see subsection 4.2.2).

4.2.1 Possibility of migrating the cryptographic functions

Long-term protection of privacy and security poses various challenges. One of these challenges is how to maintain a high level of protection by cryptographic means. It is foreseeable that today's assumed strength of cryptographic modules will not be kept of a period of several years. Instead, it will be necessary to migrate to new cryptographic algorithms or other safeguards.

This plays an important role in the privacy-enhanced backup and synchronisation system since cryptographic modules will be key components. Here the concept of the demonstrator should elaborate how a migration of the cryptographic functionality is possible and how parties involved will be informed about the necessity of migration including the potential consequences when migrating or not migrating that functionality.

Further it could be discussed whether for the sake of robustness different cryptographic means should be used in parallel. Hence, in case one of the algorithms or implementations has to be considered not safe any more, the other one would still ensure a high level of protection. However, implementing this may be too sophisticated for the purpose of a demonstrator.

4.2.2 Storing backup items in a cloud

In the current concept of the WP 1.3 demonstrator, the set of storage providers seems to be clearly defined in advance. According to the concept, the primary user can always be aware of where the backup items are located.

A different setting would be the storage of backup items in a cloud.[5] A definition of cloud computing is provided by the National Institute of Standards and Technology (NIST)[6]: "Cloud

[5] Similarly, in the FP7 project "VISION – Virtualized Storage Services Foundation for the Future Internet" it is planned to implement a "Personal Data Safe" in a cloud computing environment (cf.

computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing poses many legal challenges, especially on the issue of responsibility for the (personal) data, liability issues, the relationship between different members of the cloud (who is a data controller, who is a data processor, which contracts exist?), the applicable law and questions concerning possibly trans-border data flow. Surely it is not an unrealistic scenario, but for the demonstrator it should not be tackled because this would unnecessarily complicate its design.

4.3 Scenarios to support users

The backup and synchronisation system probably will require primary users to explicitly configure which data belongs to which partial identities and the exact delegates. There might be more convenient solutions that would require supporting mechanisms. This section describes two of those possible mechanisms.

4.3.1 Support primary users in sorting their data

Handling several partial identies for various areas of life will be not that easy for users. This will be even more difficult or at least cumbersome if they have to think of different delegates for separate areas of life. A manual configuration via the backup and synchronisation system would not be very convenient.

However, it would be possible for communication partners of the primary users including the issuers of official documents such as diploma certificates, school reports or tax IDs to attach information on how to keep them. This attached information may comprise how confidential they should be stored, how quickly they should be available, who should be able to access them under which conditions, with whom to share, how to involve delegates and inform them about their tasks concerning specific data items etc. A standardised set of metainformation that is known and interpreted by the privacy-enhanced backup and synchronisation system could be very helpful for users to sort their data and handle them appropriately.

4.3.2 Third-parties identified by role

The primary user could choose to grant access to individuals representing a role, without necessarily be identified by individual information. This could be defined as a group of several persons playing the same role, defined, e.g., by a particular position in a given organisation. It might also be automatic that the primary user, by taking a position in this organisation, delegates without having to express this delegation specifically, i.e. her own role conveys the delegation to any person fullfilling another role concerning backup items of specific partial identities. Still the user interface should clearly communicate who is able to get access.

In that matter, ontologies could be used to define classes or equivalences of roles. Then the organisation policies could include rules that would use those classes to determine the access

http://www.snia.org/cloud/JulyMiniSummit/VISION_for_SNIA_Cloud_minisummit_July_23_2009.PDF, page 11).

[6] Peter Mell and Tim Grance: The NIST Definition of Cloud Computing, Version 15, 2009, online available at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

control rights for the primary users. Again this would support users in handling their data and delegates in the backup and synchronisation system.

Chapter 5

Conclusions and outlook

After the rather abstract and very general compilation of requirements for “Privacy for Life” in the PrimeLife heartbeat H1.3.5, the concept of the privacy-enhanced backup and synchronisation demonstrator in H1.3.6 has proposed how to tackle the given requirements in such an application. This text adds second thoughts on the concept of the demonstrator: These comprise on the one hand socio-cultural requirements that have been used already in the PRIME project, on the other hand they choose relevant issues in the field of delegation as well as specific scenarios and use cases that reflect further ideas to extend the demonstrator’s perspective.

Not all of the issues and ideas in this document have led to crisp requirements that are easily implemented in a demonstrator, and for some it is even hard to decide which one is the right concept that balances the interests of the primary user, the delegates, the storage providers or other parties involved. What is more, several aspects in the area of delegation are tightly intertwined with civil law or other national regulation. Here the demonstrator should not be overloaded with a demand of solutions to all possible aspects. Still it makes sense to see the bigger picture of the backup and synchronisation service: it could be a valuable component connected to user-controlled identity management systems with support by other communication partners when they provide documents to be stored and used for a longer period of time.

We hope that our second thoughts on the current status of the WP 1.3 demonstrator help to improve it and facilitate its application for interested users.

References

[DBPK10] Dobiáš, Jaromir, Borcea-Pfitzmann, Katrin, and Köpsell, Stefan (eds.): Towards a Privacy-Enhanced Backup and Synchronisation Demonstrator Respecting Lifetime Aspects, PrimeLife Heartbeat H1.3.6, Dresden 2010, online available at http://www.primelife.eu/images/stories/deliverables/h1.3.6_final.pdf (last access: October 2010).

[GWW+10] Graf, Cornelia, Wolkerstorfer, Peter, Wästlund, Erik, Fischer-Hübner, Simone, and Kellermann, Benjamin (eds.): High-level Prototypes, PrimeLife Deliverable D4.1.4, Vienna/Karlstad/Dresden 2010, online available at http://www.primelife.eu/images/stories/deliverables/d4.1.4-high-level_prototypes-public.pdf (last access: October 2010).

[HaPS08] Hansen, Marit, Pfitzmann, Andreas, and Steinbrecher, Sandra: Identity management throughout One's Whole Life, Information Security Technical Report 13,2 (May 2008), pp. 83-94.

[HRSZ10] Hansen, Marit, Raguse, Maren, Storf, Katalin, and Zwingelberg, Harald: Delegation for Privacy Management from Womb to Tomb – A European Perspective, in: Bezzi, Michele et al. (eds.): Privacy and Identity Management for Life, IFIP AICT 320; Springer, Berlin, Heidelberg, New York 2010, pp. 18-33.

[RSLB09] Roosendaal, Arnold, Steinbrecher, Sandra, Leenes, Ronald, and Buitelaar, Hans (eds.): Analysis of Privacy and Identity Management throughout Life, PrimeLife Heartbeat H1.3.3, Tilburg 2009, online available at http://www.primelife.eu/images/stories/deliverables/h1.3.3analysis_of_privacy_and_identity_management_throughout_life-public.pdf (last access: October 2010).

[Schu08] Schumacher, Günter (ed.): Requirements for Privacy Enhancing Tools V3, Ispra 2008, PRIME Deliverable D1.1d, online available at https://www.prime-project.eu/prime_products/reports/reqs/pub_del_D1.1.d_final.pdf (last access: October 2010).

[StHR09] Storf, Katalin, Hansen, Marit, and Raguse, Maren (eds.): Requirements and concepts for identity management throughout life, PrimeLife Heartbeat H1.3.5, Kiel 2009, online available at http://www.primelife.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_life-public.pdf (last access: October 2010).