Towards a Privacy-Enhanced Backup and Synchronisation Demonstrator Respecting Lifetime Aspects

Editors:	Jaromír Dobiáš, (TUD)
	Katrin Borcea-Pfitzmann, (TUD)
	Stefan Köpsell, (TUD)
Reviewers:	Peter Wolkerstorfer, (CURE)
	Carine Bournez, (W3C)

Identifier:	H1.3.6
Type:	Heartbeat
Class:	Public
Date:	March 13, 2010

Abstract

This heartbeat deals with implications of lifelong privacy and identity management within the scope of the application area of protection against unwanted data loss. It demonstrates that there already exists an essential and useful area of a public interest – the area of backup and synchronization tools and applications – which can be enhanced by the proposed demonstrator in such a way that it corresponds to the objectives of the PrimeLife Project.

This heartbeat puts general high-level requirements elaborated in the heartbeat H1.3.5 into the context of the specific environment of the demonstrator and points out corresponding requirements and implications for the demonstrator adapted to the specific environment. It also clarifies our plans for further work, which will realize ideas of the demonstrator in the form of implementation of the core functionality and in the form of elaborated conceptual documentation.

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

Members of the PrimeLife Consortium

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

List of Contributors

The following list presents the contributors for the individual parts of this deliverable.

Chapter	Author(s)
Executive Summary	Jaromír Dobiáš (TUD)
1. Introduction	Jaromír Dobiáš (TUD)
2. Relationship between backup environment and privacy throughout life	Jaromír Dobiáš (TUD)
3. Privacy-related requirements derived from the backup and synchronization nature of the demonstrator	Jaromír Dobiáš (TUD)
4. Solutions for relevant requirements on the demonstrator	Jaromír Dobiáš (TUD)
5. Conclusion	Jaromír Dobiáš (TUD)
Appendix A	Katrin Borcea-Pfitzmann (TUD) with contributions from Sandra Steinbrecher (TUD)

Executive Summary

The technological progress of the last decades triggers transformation of our society towards a computerized social community highly dependent on information. The more structures of our society depend on information the more important is the role that data plays in our everyday lives. During decades of the technological evolution, several methods were invented storing the data in various forms and on various types of media. However, the processes and events in the nature, society, and in the life of the data subject cause failures, which might lead to loss of the data during the lifetime of the data subject. Even if unwanted data loss might not be a common phenomenon encountered within the life of every data subject, it may become an evident and serious problem, which emerges in the lifelong extent of time.

Many backup systems and backup strategies, which have been available for many years, are already dealing with the problem of unwanted data loss. However, they are mostly protecting the raw data only and do not involve the data subject, his[1] specific characteristics, social relations and interactions as a part of their scope. Existing backup systems and backup strategies also do not reflect the process of evolution of the data subject during his lifetime with respect to possible different states he might pass through during his lifetime and which might have an immense influence on his ability to manage his data on his own behalf (e.g., illness, hospitalization, or death). Additionally, existing systems and strategies dealing with the problem of unwanted data loss do not also cope with boundaries among distinct areas of the data subject's social interactions. However, these aspects are nowadays becoming more and more sensible on the level of the data, hand in hand with the massive expansion of the technology.

Therefore, we decided to analyze the problem of unwanted data loss from the perspective of lifelong privacy. We found out that current solutions do not provide a sufficient level of data protection when it comes to lifelong extent of time and privacy of the data subject holding the data. Based on our findings, we decided to demonstrate that it is possible to cope with problems amplified by the requirements on lifelong privacy when protecting the data subject against unwanted data loss.

The proposed privacy-enhanced backup and synchronization demonstrator focuses on the following problems closely linked together under the light of lifelong privacy:

1. **Protection of the data subject against unwanted data loss during his lifetime by redundancy and physical distribution of the data;**
2. **Assurance of lifelong confidentiality of the data subject's data stored in a distributed environment;**
3. **Delegation of access rights to the data subject's backup data allowing other parties to operate with his data if specific conditions are fulfilled;**
4. **Distribution of the backup data according to different areas of life of the data subject and his different partial identities.**

This Heartbeat H1.3.6 within the PrimeLife Work Package 1.3 (WP 1.3) derives requirements for the proposed WP 1.3 focal demonstrator based on the high-level requirements introduced in the Heartbeat H1.3.5 and explains how the goals of the lifelong privacy relate to the backup

[1] For the purpose of readability we refrain from using gender-neutral pronouns such as "he/she". Accordingly, gendered pronouns are used in a non-discriminatory sense and are meant to represent both genders.

environment of the demonstrator. Furthermore, it presents requirements related to privacy derived from the backup nature of the proposed demonstrator. This Heartbeat also introduces corresponding solutions derived from the presented requirements, which are relevant for the WP 1.3 demonstrator. Further, it clarifies how they will be addressed in the proposed demonstrator. Last but not least, Annex A discusses the suitability of the proposed privacy-enhanced backup and synchronization demonstrator in comparison to the prototype ideas presented within Heartbeat H1.3.4.

Contents

Chapter 1

Introduction

The objective of this heartbeat is presentation of goals of the privacy-enhanced backup and synchronization demonstrator as the third year's focal demonstrator developed in Work Package 1.3 (WP 1.3). This heartbeat clarifies requirements and solutions of the WP 1.3 demonstrator based on the high-level requirements elaborated in the heartbeat H1.3.5.

In our most recent work we determined that the primary objective of the WP 1.3 demonstrator is the protection of an EU citizen (data subject) against unwanted data loss in a privacy-enhanced way respecting lifelong aspects of the data subject. The main stimulus triggering our motivation towards this direction is that current solutions which help to overcome unwanted data loss, are dealing with only a narrow subset of existing problems usually covering limited time-frame of the data subject's life. Existing solutions however do not succeed in providing a sufficient level of protection of the data subject's data when it comes to lifelong extent of time, privacy-related aspects and semantic meaning of the content of the data with respect to the data subject and his life. This leads to new types of challenges, which need to be solved with more comprehensive approaches.

WP 1.3 demonstrator deals primarily with the following problem domains:

1. *Protection of data subject against unwanted data loss during his lifetime.*

   Our findings resulted into the conclusion that the problem of unwanted data loss can be solved by redundancy and physical distribution of multiple copies of the data from the lifelong perspective. As far as backup and synchronization tools are also dealing with the problem of unwanted data loss, we decided to establish the main conceptual pillars of our demonstrator on the backup and synchronization functionality. In the WP 1.3 demonstrator we are proposing to solve the problem of unwanted data loss by taking advantages of services provided by storage providers which are nowadays available on the Internet (for example Dropbox, Apple MobileMe, Windows Live SkyDrive, Ubuntu One and others) and store multiple copies of the data in distributed environment. Distribution of potentially sensitive backup data in such kind of environment however leads to confidentiality problems.

2. *Assurance of lifelong confidentiality of the data subject's data stored in a distributed environment.*

The problem of data confidentiality in a distributed and untrusted environment can be solved by encryption of the data. Encryption must assure that only the authorised data subject (whom the data belongs to) is able to operate with his data stored in distributed backups by default and nobody else should have implicitly access to it even after the death of the data subject. On the other hand, during the lifetime of the data subject, unpredictable situations might occur, which might temporarily or permanently limit him in his ability to access his own data (for instance in case of his illness, hospitalization or death). This might lead to situations that his data, which might be important for some other parties relying on it (possibly in a legal relationship with the data subject), is not accessible by these parties when needed (for example important work documents) or is permanently lost.

3. *Delegation of the access rights to the data subject's backup data allowing other parties to operate with this data if specific conditions are fulfilled.*

   Delegation capability of WP 1.3 demonstrator allows other parties authorised by the data subject (whom the data belongs to) to access his backup data in case that specific conditions specified by the data subject are satisfied. Delegation of access rights of the data subject's backup data could in general case lead to situations that authorised parties with corresponding access rights are not only able to access the desired data but also other data possibly covering other areas of the data subject's life, which they are not authorised to. This might however not be desired by the data subject himself.

4. *Distribution of the backup data according to different areas of life of the data subject and his different partial identities.*

   Distribution of the backup data according to particular areas of the data subject's life or his different partial identities enables the data subject to manage his privacy in such a way which allows him to physically and logically separate his data related to distinct domains of his social interaction.

Besides the above mentioned problems, additional non-trivial issues must be addressed which are covered by the high-level requirements on prototypes developed within the PrimeLife project. As far as the demonstrator is based on the backup and synchronization functionality, it has to address also further privacy-related issues amplified by the backup and synchronization nature. These aspects are covered in this document.

This heartbeat consists of five chapters:

This introduction chapter presents the objectives of this heartbeat. It depicts problem domains of the WP 1.3 demonstrator and introduces the basic terminology used in the subsequent chapters. Chapter 2 serves as the basis of requirements relevant to WP 1.3 demonstrator. It describes concrete requirements for the demonstrator derived from high-level requirements elaborated in heartbeat H1.3.5. Chapter 3 outlines additional privacy-related requirements derived from the backup and synchronization nature of the demonstrator. Chapter 4 presents solutions for requirements described in Chapter 2 and Chapter 3. Chapter 5 concludes and summarizes the results of this heartbeat.

In order to be able to correctly understand the content covered by this heartbeat it is necessary to get familiar with the following terminology, which is used in the following chapters of this document:

Terms:

- **Primary item**: an original item for which one or more backup items are created during the back up action. In a general sense, a primary item can be referred to as any determinate set of

data, which has one or more copies called backup items dedicated for backup purposes. A primary item can be a file but it can also be a more specific type of data as for instance an e-mail, a contact, or even settings of the TV.

- **Backup item**: a copy of a primary item stored in the backup. A backup item reflects the data of a primary item in the time when the backup item is created. Note that even if each backup item must belong to one and only one primary item, this primary item may not exist during the whole lifetime of the backup item. A backup item can exist in several versions in a particular point of time. The previous versions of a backup item backed up in the past are called predecessors of a backup item. Any version which is older than the current version of a backup item is considered to be its predecessor. Future versions of a backup item which will be created in the future are called successors of a backup item. All versions of a backup item which are created after the current version are considered to be its successors. Current version of a backup item is the last version which exists in the current time.
- **Backup**: a non-empty set of backup items.
- **To back up**: the process of creating copies of the primary item into one or more backup items and storing them in a corresponding storage.
- **Backup recovery/restoration**: the process of extracting an original primary item from a corresponding backup item, which was previously created during the back up process. The outgoing primary item gained from a backup recovery/restore process has the same state as the previous state of that primary item when the back up process was performed on it.
- **Storage**: physical or logical device providing storage space for the backups of the primary user.
- **Storage area**: destination where the storage is located. In our demonstrator this is mostly remote location administered by a particular storage provider accessible to the primary user and delegates virtually via communication network.
- **Area of life (AoL):** sufficiently distinct domain of social interaction that fulfils a particular purpose (for the data subject) or function (for society).
- **Stage of life (SoL):** a stage of life of an individual with respect to handling his privacy is a period in the life of this individual in which the ability to manage his private sphere remains between defined boundaries characterizing the current stage of his life.
- **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).
- **Full lifespan:** the range of time from the emergence of the first information that is related to the human being (from the moment of birth until the death of the data subject) until the point in time when no more personal data is generated.

Actors:

- **Primary user**: data subject who owns/holds primary items.
- **Backuper**: initiates the back up action. In most applications of this demonstrator, the primary user acts as the backuper.
- **Restorer**: participates on the backup recovery/restoration action and obtains the content stored in a particular backup as the result of successful backup recovery/restoration action.
- **Deleter**: initiates the delete action on a particular backup. In most applications of this demonstrator, the primary user acts as the deleter.
- **Storage provider**: provides storage space for backups.
- **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.
- **Legally related party**: is anyone being in a legal relationship with the primary user or the storage provider.
- **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.
- **Attacker**: is an entity, which performs malicious activities trying to violate mechanisms of the privacy-enhanced backup and synchronization demonstrator. These are mostly activities, which can lead to the achievement of unauthorised access rights to the backup data, which can cause damage or unauthorised modification of the backup data or unauthorised damage or modification of the relation between the backup and the involved third party (mostly primary user). Further activities of the attacker also cover unauthorised linkage of the backup data, which was intentionally separated (physically or/and logically), or unauthorised linkage of the actions of the primary user or involved third parties performed on the backup. Last but not least, activities of the attacker are also those actions which have unwanted impact on the mechanism of conditional access control and which are not authorised by the primary user.

Chapter 2

Relationship between backup environment and privacy throughout life

This chapter clarifies relation between the backup environment and goals of privacy throughout life which are coupled in WP 1.3 demonstrator. High-level requirements, which were elaborated in heartbeat H1.3.5 [SHR2009], serve as the basis for this chapter. These requirements are transformed and adapted into a more specific form in this chapter in order to reflect the nature of the application area of the demonstrator.

2.1 Transparency

Transparency plays an important role in many areas of our society. In general, transparent behaviour among particular subjects allows those subjects to be informed about activities, actions, results, and other relevant information related to the corresponding subjects behaving transparently. Transparency brings openness, clearness and controllability to relations among interacting subjects. Transparency plays an essential role in those situations, where data processing is being performed such that certain parties are coming in contact with the data related to other parties. It is therefore necessary to consider transparency as one of the key aspects of the WP 1.3 demonstrator.

I. The first high-level requirement stated in the heartbeat H1.3.5 is transparency. It says that [H1.3.5, Sec. 3.1.1]:

> *"For all parties involved in privacy-relevant data processing, it is necessary that they have clarity on the legal, technical, and organisational conditions setting the scope for this processing (for example, clarity on regulation such as laws, contracts, or privacy policies, on technologies used, on organisational processes and responsibilities, on data flow, data location, ways of transmission, further data recipients, and on potential risks to privacy).*"

In terms of the WP 1.3 demonstrator, this requirement can be rephrased to the following form:

For all parties involved in the back up, recovery, delegation of access rights, or which provide storage for the backup as well as other third parties involved in the privacy-enhanced backup and synchronization demonstrator schema, it is necessary that they have clarity on the legal, technical and organisational conditions setting the scope of their role with respect to the data or privilege corresponding to their role (for example, clarity on regulation such as laws, contracts, or privacy policies, on technologies used, on organisational processes and responsibilities, on data flow, data location, ways of transmission, further data recipients, and on potential risks to privacy).

The indicated requirement on transparency can be further extended into more specific sub-requirements specified on the level of concrete actors of the privacy-enhanced backup and synchronization demonstrator:

Above all, it is necessary that the primary user becomes familiar with the basic technical background of the distributed backup schema and also with potential risks that are amplified by the nature of the distributed environment. The primary user must be familiar with protection mechanisms (existing on the technical as well as legal level), which protect his data. He must also be able to learn what the services are and guarantees provided by a storage provider and, under which conditions and to what extent, the storage provider provides his services especially when it comes to lifetime aspects and the death of the primary user. It must be clarified that if the primary user takes advantage of services of an external storage provider, he fully relies on the storage space provided by the particular storage provider and his technical equipment, which is not under the physical control of the primary user. The primary user must also understand what are the potential risks and privacy implications when he enables other parties to restore his backup in case that a specific condition is satisfied.

II. The transparency requirement is also elaborated from the scope of revocability and irrevocability. In heartbeat H1.3.5 [H1.3.5, Sec. 4.1.2], it is stated that:

> *"For all parties involved in privacy-relevant data processing, it should be clear under which circumstances decisions are revocable/irrevocable and what the potential impact can be. In particular, data controllers should inform data subjects on to which degree their decisions (such as consent to processing of personal data or distribution of these data) are revocable or not."*

This high-level requirement can be adapted to the following form fulfilling the scope of the backup environment:

- For all parties involved in the back up, recovery, delegation of access rights, or which provide storage for the backup as well as other third parties involved in the privacy-enhanced backup and synchronization demonstrator schema, it should be clear under which circumstances their actions are revocable/irrevocable and what can be the potential impact. In particular, the primary user should be informed what his possibilities to revoke access rights from corresponding delegates are and what impact does a particular deletion action have on the backed up data. The primary user must also be informed about possible ways of deletion of his backup data and about corresponding implications of particular types of deletion. He must further be aware that he can always delete whichever item of his backup data in all existing instances (even older copies of some item) and in all backup locations under control of the primary user. It must be clarified what happens to the backup data on the storage provider's site. It must be explicitly specified if the storage provider utilizes some backup mechanisms and strategies also on the server side and what impact does it have on the primary user's data in case he deletes his backup items or cancels his contract.
- A delegate must be aware of his possibility to refuse access rights delegated by a delegator in any point in time and the delegator must be informed about it as soon as possible.

- Storage providers must be aware of their possibility to cancel the contract with a primary user in case that the primary user violates conditions defined by the storage provider, which are accepted by the backuper during his subscription.

III. Further requirements on the transparency are [H1.3.5, Sec. 4.1.5]:

> *"Data controllers and data processors should make transparent for data subjects, under which conditions (potentially) personal data may be, will be or actually are linked."*

With respect to the privacy-enhanced backup and synchronization demonstrator, this high-level requirement means:

The primary user must be informed that, by delegating access rights to several delegates, his areas of life can be linked [PfHa2009] together. He must also have clear control about which data can be linked under which conditions. The primary user must be aware of the possibility of linkage of his operations performed on distributed backups. He must be informed which functionality can be provided by using anonymisation service and how it can help him to avoid linkability and other related problems.

IV. The next requirement, which deals with the case of privacy and security breach [H1.3.5, Sec. 4.1.6], says:

> *"Data controllers and data processors should inform data subjects concerned and supervisory authorities timely on privacy and security breaches and give advice on how to cope with the (potential) consequences."*

In terms of the backup and synchronization demonstrator, this requirement can be interpreted in two adapted formulations as follows:

- In case that some attack method on any security mechanism, which is used in the backup and synchronization demonstrator, appears or any security function, which is used in the schema, is considered to be unsecure, the primary user must be informed about existing risks with respect to potential consequences on the privacy and security of his data and provided advice on how to cope with this problem.
- In case of a successful attack on the storage provider, the primary user must be informed about this incident and about possible consequences with respect to his data and how to deal with these consequences.

2.2 Data minimisation

Further high-level requirements elaborated in heartbeat H1.3.5 are related to data minimisation. The principle of "data minimisation" says that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. A data controller should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only that personal data they really need, and should keep it only for as long as they need it [Euro1995].

I. In the heartbeat H1.3.5 data minimisation is defined as follows [H1.3.5, Sec. 3.1.2]:

> *"Data minimisation means to minimise risks to the misuse of these data. If possible, data controllers, data processors, and system developers should totally avoid or minimise as far as possible the use of (potentially) personal data, conceivably by employing methods for keeping persons anonymous, for rendering persons anonymous ("anonymisation"), or for aliasing ("pseudonymisation"). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If (potentially) personal data cannot be avoided, they should be erased as early as possible. Policy makers should implement the data minimisation principle in their work, be it in law making or technological standardisation."*

In the privacy-enhanced backup and synchronization demonstrator, this requirement pertains to storage providers and delegates and can be phrased as the following:

- The possibility of the storage provider to observe or link actions of the primary user must be avoided or minimised to an acceptable level. This means that a particular storage provider should not implicitly be able to learn the real identity of the primary user. The primary user should not use the same personal identifier for different storage providers because this could lead to linkability of the user's actions especially in case if two or more storage providers are controlled by a single entity.
- Delegates should be able to perform selected operations authorised by the primary user on his backup in case that all access conditions predefined by him are fulfilled. Any delegate should however not be able to link or observe actions of the primary user (backuper, respectively). In particular delegate should implicitly not be able to link or observe actions covered by diverse areas of life of primary user or his partial identities. The primary user should be able to keep his areas of life separated and link them only in cases he explicitly wants to link them for one or more selected delegates.
- An attacker must not be able to observe actions of the primary user (backuper, respectively) performed on the backup stored in the distributed environment (on storage provider's equipment). An attacker must not be able to link actions performed by the primary user, which means that he cannot learn that two actions performed on one particular backup were initiated by the same primary user.

II. The principle of data minimisation further requires minimal quantity and sensitiveness of the data controlled by third parties. Heartbeat H1.3.5 namely says that [H1.3.5, Sec. 4.2.1]:

> *"Data controllers and data processors, and system developers should minimise the storage of (potentially) personal and sensitive data as far as possible."*

Under the scope of the privacy-enhanced backup and synchronization demonstrator, this requirement relates to storage providers and delegates. It can be interpreted in the following way:

- Storage providers and delegates should have only minimal access to personal and sensitive data of the primary user. As far as the role of storage providers is to provide remote storage space for backups of the primary users only, they have no reason for accessing the content of the primary user's data. Therefore, according to the principle of data minimisation, storage providers should not be allowed to access the backup data of the primary user. They should operate only with such a type of data, which is necessary for providing their services and accounting. This means that confidentiality of the backup data has to be assured as far as the data is stored in a storage space provided by storage provider.
- The access of delegates to the primary user's backup should be minimised to such an extent, which is wanted and expected by the primary user. The primary user should minimise the access of selected delegate(s) to specific backup data by appropriate access conditions. If the

primary user decides to minimise access to his backup data by using access conditions, selected delegates are allowed to access the backup data only in case they provide the corresponding credentials issued by credential issuers, which proves that the access conditions are fulfilled.

III. Moreover, the need to minimise quantity and sensitiveness of the data handled by involved parties is extended in the following definition of the heartbeat H1.3.5 [H1.3.5, Sec. 4.2.1]:

> *"Supervisory authorities and privacy organisations should support individuals, data controllers and data processors, and system developers to fulfil the principle of data minimisation by giving advice concerning concepts and implementations, pointing to best practices and support research and development in this field. This may be done by employing methods for keeping persons anonymous, for rendering persons anonymous ("anonymisation"), or for aliasing ("pseudonymisation"). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If (potentially) personal data cannot be avoided, they should be erased as early as possible."*

In terms of the privacy enhanced backup and synchronization demonstrator, this requirement means that security mechanisms, which assure unobservability and unlinkability of the primary user's actions as well as anonymisation and pseudonymisation of the primary user's identity, must be supported by the demonstrator. In case that a storage provider needs to hold some personal data of the primary user for providing his services, this data must be erased as early as possible.

IV. A further requirement on data minimisation deals with the time frame of storage of the data. In heartbeat H1.3.5 it is stated that [H1.3.5, Sec. 4.2.2]:

> *"Data controllers and data processors, and system developers should minimise the time frame of storage and use of (potentially) personal data as far as possible. After that time, the data should be fully erased. This should comprise temporary files or data which have been distributed to other media or recipients as far as possible."*

Adapted to the privacy-enhanced backup and synchronization demonstrator, this requirement means that:

- Every delegate who was given access rights determined by access conditions must be allowed to access the data only within the duration of validity of the particular access conditions and for the specific purpose of access rights. This means that as soon as the access conditions are no longer valid, the delegate must not longer be allowed to perform permitted operations on the backup data of the primary user with respect to the particular access conditions.
- From the storage provider's point of view, this high-level requirement obliges the storage provider to minimise the time frame of holding personal data of the primary user with respect to the duration of the contract between the storage provider and the primary user. After this period of time, which must be defined within the terms and conditions and accepted by the primary user, the storage provider must implicitly and immediately erase any identifier or information, which leads to identification of primary user and his backup data as well.

V. Section 4.2.3 of the heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.2.3]:

> *"Data controllers, data processors as well as individuals should minimise the disclosure of (potentially) personal data as far as possible."*

For the privacy-enhanced backup and synchronization demonstrator, this requirement relates to storage providers, delegates and credential issuers. All these actors must minimise the extension of personal data to that level, which is necessary for fulfilling the specific purpose. For example, a primary user (delegator, respectively) should delegate access to only that data which fulfils the purpose of the delegation. This implies that an appropriate access condition should be selected by the primary user (delegator, respectively) according to the purpose of the delegation. In any case, the primary user must be aware of the fact that as soon as the delegates gain access to his data, the primary user (delegator, respectively) has to rely on the trustworthiness of the delegates because in fact he has no longer direct control on what actually happens to his data. Also backup data, which may contain personal data of the primary user, should not be disclosed to storage providers or any other third party if not authorised by the primary user (delegator, respectively).

VI. Section 4.2.5 of heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.2.5]:

> *"Data controllers and data processors, and system developers should minimise linkability and linkage of (potentially) personal data as far as possible."*

Within the scope of the privacy-enhanced backup and synchronization demonstrator, this requirement applies mostly to the primary user. The primary user should minimise linkability and linkage of his actions and data by using suitable tools assuring unlinkability, which must be supported by the demonstrator. Above all, linkability should be avoided between different areas of life and different partial identities of the primary user.

> *"Data controllers and data processors, and system developers should minimise multipurpose or context-spanning use of (potentially) personal data as far as possible. They should provide mechanisms for context separation of these data."*

For the privacy-enhanced backup and synchronization demonstrator, this high-level requirement means that the demonstrator must provide mechanisms, which minimise multipurpose or context-spanning use of (potentially) personal data stored in the backup or stored by the storage provider for accounting purposes. In particular it means that storage providers, attackers or other third parties (legally related or not) are not able to use potentially personal data of the primary user for different purposes.

> *"Data controllers and data processors, and system developers should avoid the use of unique identifiers which may be used in different contexts. They should use diverse identifiers where possible."*

Within the scope of the privacy-enhanced backup and synchronization demonstrator, that means that the demonstrator must avoid using unique identifiers in different contexts. A primary user's accounts provided by different storage providers must use diverse identifiers. Any two backups, which were created for different purposes, must also be stored under different accounts using diverse identifiers.

> *"Data controllers and data processors, and system developers should support anonymous or pseudonymous authorisation and access control of users where possible."*

In terms of privacy-enhanced backup and synchronization demonstrator, this requirement mostly relates to storage providers. Storage providers should support anonymous or pseudonymous

authorisation and access control of users where possible. Pseudonymous authorisation and access control should also be supported between primary user (delegator, respectively) and delegates as well as between delegates and corresponding storage provider.

VII. Section 4.2.6 of the heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.2.6]:

> *"Data controllers and data processors, and system developers should minimise irrevocable consequences concerning the privacy of data subjects."*

For the privacy-enhanced backup and synchronization demonstrator, interpretation of this requirement leads to the following two requirements adapted for the environment of the demonstrator:

- The primary user (respectively delegator) should always be able to revoke access rights delegated to delegates.
- The primary user should always be able to remove any backup item contained in any backup he created including older backup items of the same primary item.

2.3 Fair use – Controllable and controlled data processing

I. In heartbeat H1.3.5, it is stated that [H1.3.5, Sec. 3.1.3]:

> *For all parties involved in privacy-relevant data processing, the processing should be controllable and controlled throughout the full lifecycle. It should be compliant with the relevant legal and social norms.*

From the point of view of the privacy-enhanced backup and synchronization demonstrator, this high-level requirement concerns storage providers and credential issuers. Processing by the storage provider as well as by the credential issuer should be controllable and controlled throughout the full lifecycle and it should be compliant with the relevant legal and social norms.

II. Heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.1]:

> *"Data controllers and data processors should restrict the processing of (potentially) personal data to a predefined purpose."*

According to the specific purpose of the demonstrator, this requirement should assure that the demonstrator provides appropriate mechanisms, which allow the primary user to easily separate his data and create a backup corresponding to the specific purpose respecting potential risk factors during the lifetime of the primary user.

III. Heartbeat H1.3.5 also requires that [H1.3.5, Sec. 4.3.1]:

> *"Data controllers and data processors should be specific in the definition of the respective purposes."*

Within the scope of the privacy-enhanced backup and synchronization demonstrator, storage providers should be specific in the definition of what kind of information is required in order to support accounting and anonymous payment. In case that there are some third parties to whom a

storage provider provides information about his clients, this must be explicitly mentioned to the primary user including the purpose for which this information is provided and what the potential consequences are.

IV. Heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.2]:

> *"If the data processing is based on consent: Data controllers should limit the data subject's consent in time by default."*

Under the light of the demonstrator, this requirement can be transformed into the requirement that every access right should include a reasonable validity period by default.

V. Heartbeat H1.3.5 additionally requires that [H1.3.5, Sec. 4.3.2]:

> *"If the data processing is based on consent: Data controllers should ensure that the data subject can withdraw the consent without unexpected impacts on his privacy (because of irrevocable consequences)."*

Adapted to the special environment of the demonstrator, this requirement means that a primary user (respectively delegator) should be able to revoke access right delegated to one or more delegates. On the other hand, the backup and synchronization demonstrator does not allow the primary user to permanently remove any data, which was provided this/those delegate/delegates by delegation of the access right.

VI. Heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.2]:

A primary user should be able to make the delegate accountable. The primary user should be able to define and assign clear responsibilities, which must be clear to the delegate before he accepts the delegation of access rights.

VII. Heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.2]:

> *"Data controllers and data processors should prohibit identity theft, especially in situations which may have privacy-infringing impacts."*

- The primary user (delegator, respectively) should prohibit identity theft by not delegating access rights of the backup data to delegates who are not trustworthy regarding the specific purpose of the backup. Sensitive data should be distributed and protected in such a way that no unauthorised person is able to access it.
- Primary user should also avoid identity theft by not providing his real identity to any storage provider if not necessary. This means that there should be a mechanism which allows the user to communicate with storage providers anonymously or at least pseudonymously.

VIII. Another requirement of heartbeat H1.3.5 says that [H1.3.5, Sec. 4.3.3]:

> *"Data controllers and data processors should conceptualise and plan their privacy-relevant data processing beforehand, thereby covering the full lifecycle of data (from creation to deletion). This comprises to plan the process and set the conditions for potential or factual linkage of data and – if the data processing is based on consent – also for its revocation."*

A primary user (delegator, respectively) should conceptualise and plan his backup recovery strategy resulting in the corresponding access rights and conditions before the access rights are delegated to delegates. During the creation of a new backup, the demonstrator should provide the possibility to define the time period in which backup items are automatically updated on a regular basis. In case that the primary user (backuper, respectively) does not specify a time period for backup updates explicitly, the demonstrator should ask the primary user (backuper, respectively) if a corresponding backup should be updated in case that some primary item was modified.

IX. Additional requirement of heartbeat H1.3.5 says that [H1.3.5, Sec. 4.3.3]:

> *"If identifiers are created, data controllers and data processors should already foresee concepts and procedures for their erasure after the usage period."*

This requirement can be adapted to the formulation that, in case that there are some identifiers created (for instance for the purpose of accountability by storage providers), there should already be concepts and procedures, which assure that those identifiers are erased after the usage period.

X. Further requirement of heartbeat H1.3.5 says that [H1.3.5, Sec. 4.3.3]:

> *"Data controllers and data processors should also plan for emergency situations (for example, privacy and security breaches)."*

Primary users as well as storage providers should be prepared for emergency situations. For a storage provider, this could, e.g., be an unrecoverable damage of a storage medium. For the primary user, this could, e.g., be a loss of connection during the backup procedure or appearance of an attack method, which defeats some security mechanism which the demonstrator relies on.

XI. Heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.3]:

> *"Data controllers should prevent lock-in situations. For example, SNS providers should provide portability for user profiles."*

- Lock-in situations should be expected and prevented by the demonstrator. For example in case that a particular storage provider does not provide stable services or is temporarily out of service, the demonstrator should allow the primary user to easily migrate his backups to some other storage provider allowing corresponding delegates to still have access to the backup data. This means that there should be a mechanism, which allows the primary user (backuper, respectively) to move his backup data stored by a particular storage provider to a storage space provided by another storage provider. In a simple setting of the demonstrator, this should be achieved by downloading the backup data directly (if possible) or from corresponding redundant copies of the backup data stored by other storage providers (in case that the affected storage provider is not able to provide access to primary user's data) and subsequently uploading the data to storage provided by the other storage provider. In a more advance setting of the demonstrator, it should be possible to realize direct upload from storage provider(s) to another one without the need to download the data to the primary user's side before uploading it. In any case it must be assured that actions performed during the migration are not linked to each other. The "receiving" storage provider should not be able to learn that the incoming data is coming from the "sending" storage provider and the "sending" storage provider should not be able to learn that the data is sent to the other storage provider as well. The migration mechanism must assure that the information about the current location of delegated backups is updated accordingly after the upload of the backup is finished. In a more

advanced setting, the update of the current location of the backup should not require active participation of the corresponding delegates having rights to perform particular actions on the migrated backup.

XII. Heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.3]:

> *"Data controllers, and in SNS also peers, should clearly define responsibilities in case of joint responsibility of data as well as the rules for jointly or separately using the joint data (for example, in a (privacy) policy or another binding contract)."*

Storage providers should clearly define internal responsibilities and rules for its staff members, especially in case that this particular storage provider relates on equipment, which is physically separated in distributed storage facilities around the world.

XIII. Sections 4.3.4 of the heartbeat H1.3.5 requires that [H1.3.5, Sec. 4.3.4]:

> *"Data controllers and data processors should be extra cautious with (potentially) sensitive data."*

This requirement can be adapted into the following form:

- A primary user (delegator respectively) should be extra cautious when delegating access rights to delegates especially in case that the backup for which the access rights are delegated contains sensitive data of the primary user. Delegates should be extra cautious when accessing the backup data delegated by the primary user (delegator, respectively). This holds especially in such cases when a delegate is bound by a legal agreement (for example non-disclosure agreement).
- Storage providers should provide such mechanisms and policies which do not allow any unauthorised third party to access the potentially sensitive data of the primary user (backuper, respectively).

2.4 Consent and revocation

Heartbeat H1.3.5 requires that [H1.3.5, Sec. 3.1.3.1]:

> *"In general, users' data should only be accessible to authorised third parties. These include parties that are legally allowed to access the information (secret service, descendants, doctors), or that have been given consent by the data subject. Given the large time frame, data subject's consent should be limited in time by default (for example, the consent given by parents for their children is limited until children reach legal age and become autonomous to decide about the consent)."*

In terms of the privacy-enhanced backup and synchronization demonstrator, this requirement applies to primary users (delegators, respectively) and their possibility to delegate access rights of their backup data to other delegates. If it is possible, validity of the access rights delegated by the primary user (delegator, respectively) should be limited in time by default according to the purpose of the backup. For example, access rights delegated to a company, which employs the primary user, should be valid only for the period of time for which this primary user is working for that particular company.

2.5 Usability

I. In heartbeat H1.3.5, it is stated that [H1.3.5, Sec. 4.1.1]:

> *"Data subjects should be made aware of potential risks to privacy and ways to deal with these risks, for example, in privacy policies."*

For the primary user of the privacy-enhanced backup and synchronization demonstrator, it means that he should be made aware of potential risks to privacy especially in a case that he stores some data in a distributed environment and in case that he delegates access rights of his backup data allowing other entities to operate with this data.

II. Heartbeat H1.3.5 says that [H1.3.5, Sec. 3.2.6]:

> *"Another aspect is the evolution of a user experience over the full lifespan of the data subject. 'Unambiguous human-machine communication' is crucial to keep the elderly and people with low education as long as possible able to act on their own behalf."*

This means that the backup and synchronization demonstrator must provide interfaces, which adhere to common usability principles reflecting the specific needs and characteristics of its individual users.

Chapter 3

Privacy-related requirements derived from the backup and synchronization nature of the demonstrator

In the previous chapter, adapted forms of requirements for the privacy-enhanced backup and synchronization demonstrator were derived from the high-level requirements provided by heartbeat H1.3.5, which themselves serve as the basis for developing and testing PrimeLife prototypes dealing with lifetime aspects. Additional privacy-related requirements stemmed from the specific backup and synchronization nature of the demonstrator are introduced in this chapter. These requirements come up due to two main reasons:

- Backup data of the primary user of the demonstrator is stored primarily in a distributed environment and in redundant copies in order to deal with the problem of data loss during the lifetime of the primary user.
- Other parties can operate with potentially sensitive content of the backup data, which belongs to the primary user in case predefined specific circumstances are fulfilled.

3.1 Location of the backup data

The more storage space on different storages located in diverse storage areas is available to the backup and synchronization demonstrator the more robust behaviour of the demonstrator can be achieved. Sufficient amount of distributed storage space enables the demonstrator (or primary user) to create more redundant copies of the primary user's data and also provides more possibilities for separation of different areas of his life and partial identities. However, as far as the amount of data stored in different distributed locations increases, the primary user might lose control over the location of his backup items.

Therefore, the primary user must be able to know what data is stored in which of his backups. He must also have some mechanism, which allows him to visualize which of his existing primary items are backed up so that he has a clear idea which of his data has already been backed up and where. The primary user should also be able to search his backup items based on selection of certain criterions (e.g., based on areas of life, partial identities, date of creation, stage of life when the item was created, name of the item, and others). The primary user should also be able to detect

those backup items for which an original primary item no longer exists. When searching for a file or performing any other localization action, any potential attacker must not be able to learn what backup data the primary user or delegate (fulfilling all access conditions) is searching for, in which backup is that particular data stored or even that he is performing a search action. Attacker should also not be able to link a user's identity with the location of the user's backups.

3.2 Backup and removal of a single item

The primary user should be able to insert (respectively delete) a single item to (respectively from) an existing backup. The application of this requirement should assure that the primary user can effectively operate with backups stored in the distributed environment. When performing the operations *insert* or *delete* on a single item, any potential attacker must not be able to reveal the content of the item inserted or deleted by primary user, what backups are influenced by this action or even that an insert or delete action was performed. Any potential attacker should not be able to reveal any of the backups stored by particular storage providers.

3.3 Back-in-time recovery

The primary user (backuper, respectively) should be able to create a backup that allows him to recover previous versions of one or more backup items reflecting the previous state(s) of the corresponding primary item. This means that the primary user (backuper, respectively) should not only be able to recover the last state of the primary item archived by the most recent back up action but also any previous state of that particular primary item created by backing up the item in the past. This functionality should allow the primary user to return back in time and restore previous states of primary items. Previous versions of primary items must be handled in the same way as ordinary backup items when performing some actions on the backups so that the same level of privacy is assured for all backup items.

When delegating access rights, the primary user (delegator, respectively) should be able to specify whether the delegate (restorer, respectively) should be able to access all versions of a particular backup item (the most recent version and all previous versions created in the past) or only a selected subset of versions of a backup item (e.g., delegate access rights to all versions of the backup item which will be created within next two weeks). The primary user (delegator, respectively) should also be able to delegate access rights to a particular version of a backup item and all of its successors (even those which do not exist in the time of the delegation) or to a particular version of a backup item and its predecessors.

The backup, which stores previous versions of the backup items, might generally reveal more information about the primary user than a simple backup storing the most recent versions only because the former contains the primary user's data spanning a broader time frame. Therefore, it is necessary to consider the fact that, once the backup contains data covering long-term history of the backup items, it becomes more valuable for potential attackers. Thus, advanced security mechanisms assuring privacy of the backup data should be utilized by the demonstrator.

3.4 Full deletion

The primary user (deleter, respectively) should also be able to completely delete all backup items created for a particular primary item by using the "full deletion" function. This means that as soon as the "full deletion" is activated on some backup item, all related backup items corresponding to the same (possibly no longer existing) primary item must be deleted. This also includes related backup items stored in different backups of the primary user (stored by different storage

providers) as well as older versions of backup items in case of back-in-time recovery function activated. Full deletion of a backup item must assure that for a selected backup item all of its existing forms (including different versions) are erased from all backups and there is no evidence that it was ever stored in any of the user's backups. This function enables the primary user to delete any backup item at any point in time. This function must enhance the primary user's privacy so that, after activation of the full deletion, he is sure that all copies of that particular backup item stored in any of his backups are deleted (even those stored in a backup device of the storage provider in case that the storage provider backs up the client data by default on the server side). The full deletion must be applicable to all backup items, which enables the primary user (deleter, respectively) to delete all of his backup data. The process of full deletion must be compliant with the requirements on privacy, anonymity (and pseudonymity) of the primary user and unlinkability of his actions, partial identities, and areas of life. Full deletion supports the primary user in his possibility to "start over", which is discussed in heartbeat H1.3.5 (see [H1.3.5, Sec. 4.3.5]).

3.5 Backup recovery after unrecoverable crash of the user's system

The primary user must be able to recover all of his backup data stored in all of his backups. For example even in a case that the computer of primary user burns and all the local data is permanently lost, he should be able to recover all of his backup items possibly on a different system.

Chapter 4

Solutions for relevant requirements on the demonstrator

This chapter presents solutions for relevant requirements introduced in Chapter 2 and Chapter 3 of this heartbeat. Furthermore, this chapter draws the line between solutions, which will be directly implemented and demonstrated and those which will be solved only conceptually in the form of written specifications.

Some requirements introduced in Chapter 2 are not included in this chapter. Rather only those which are directly relevant for our demonstrator from the implementation point of view and which can be really demonstrated as the real privacy-related solutions by our demonstrator are included. This means that requirements which are not directly covered in this chapter are, on the one hand, already covered by other sections of this chapter, or on the other hand, they have only general impact and cannot be directly demonstrated in the form of implementation in our demonstrator. These requirements might however serve as relevant and reasonable concepts for more advanced versions of our demonstrator which can for instance lead into privacy-enhanced improvements of storage providers' services and thus provide further concepts for comprehensive privacy-enhanced environment as the scope of further work.

Solutions presented in this chapter are elaborated on a high-level approach, not currently describing concrete detailed technological details of the final demonstrator. More concrete technical and implementation details as well as the according mechanisms will be focused on in further work on the demonstrator.

4.1 Solutions for transparency requirements

This section introduces solutions which fulfil requirements on transparency introduced in the section 2.1 of this heartbeat. The main goal of the "transparency" in general social context is to provide openness, disclosure, awareness or accountability. In this section solutions for the demonstrator based on transparency requirements are presented.

4.1.1 Solutions for openness, transparency, notice, awareness, understanding

The first requirement adapted for our demonstrator which is presented in subsection I of section 2.1 in this heartbeat [H1.3.6, Sec. 2.1, Part I.] requires that it is necessary that the primary user becomes familiar with basic technical background of the distributed backup. Moreover, he should be informed about potential risks of the backup environment and corresponding protection mechanisms as well as conditions, under which storage providers offer their services.

Solutions for the demonstrator:

In our demonstrator, this requirement will be solved by stating this information in the *End User License Agreement* (EULA), which will have to be accepted by the primary user before the installation proceeds. Furthermore, this information will also be presented in the start-up window in an interactive way introducing the above-mentioned information in several well-structured steps. After that, it will also be possible to open an introductory information window by activating the corresponding menu item at any time during the user's work. There will also be a wizard, which will provide the user necessary information related to the action, which the user plans to perform, and warn him about possible consequences in case the action of the primary user might have an impact on his privacy with respect to his areas of his life or partial identities.

Integration in the demonstrator:

These solutions will be addressed in the form of conceptual specification in the demonstrator.

4.1.2 Solutions for transparency of what is irrevocable and what is revocable

Subsection II of the section 2.1 of this heartbeat requires that particular actors playing their specific roles in the demonstrator's environment should have clearness under which circumstances their actions are revocable and irrevocable (see [H1.3.6, Sec. 2.2, Part II.] for details).

Solutions for the demonstrator:

In our demonstrator this requirement will be solved for primary users, delegates and storage providers. If the primary user (or delegator, respectively) wants to delegate access rights to any of his backups he is informed that he can revoke these access rights anytime in the future. He is also informed that in case that any delegate fulfils all conditions for accessing primary user's backup data, this data can be irrevocably copied and stored by the delegate. The primary user (delegator respectively) is asked if he understands possible risks and consequences of the delegation and if he really wants to delegate selected access rights which enable selected third parties to perform selected operations on the selected backup data in case that selected access conditions are satisfied. Delegation of access rights proceeds after the primary user (delegator, respectively) confirms it.

Third parties are becoming delegates of a particular backup data if they accept a delegation request. Before accepting, every delegate candidate is informed 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 refuse (revoke) delegated access rights anytime in the future if he accepts it.

Storage provider should be able to cancel the contract in case that primary user (backuper, respectively) violates conditions of storage provider. In the demonstrator there is an interface which informs primary user (backuper, respectively) that storage provider cancelled the contract

due to specific reason and gives primary user (backuper, respectively) advice how to reallocate backup data.

Integration in the demonstrator:

These solutions will be addressed in the form of conceptual specification in the demonstrator.

4.1.3 Solutions for transparency on linkage and linkability

Subsection III of the section 2.1 of this heartbeat requires, that primary user must be aware of the risk of linkage and linkability of his actions, data, areas of life and others (see [H1.3.6, Sec. 2.2, Part III.] for details) when operating with the demonstrator and he must be provided adequate information on how to avoid this risks.

Solutions for the demonstrator:

In our demonstrator this requirement will be solved by informing the primary user (delegator, respectively) that his areas of life or partial identities will be linked together if selected access rights will be delegated to selected delegate candidate. Demonstrator will also inform primary user (delegator, respectively) under which conditions linkage will occur in case that delegate candidate receives access rights. Delegation request will be sent to delegate candidate only when primary user (delegator, respectively) confirms that he is aware of potential risk of linkage of his areas of life (or partial identities).

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator.

4.1.4 Solutions for privacy and security breach notification

Subsection IV of the section 2.1 of this heartbeat requires, that in case of a security breach of some security mechanism integrated to the demonstrator or in case of security incident of any storage provider the demonstrator derives benefit from there should be some mechanism which informs the user about this incident and possibly gives him advice on how to cope with it (see [H1.3.6, Sec. 2.2, Part IV.] for details).

Solutions for the demonstrator:

In our demonstrator first requirement will be solved by detection mechanism which monitors possible breaches of security functions utilized by the demonstrator. Second requirement will be solved by communication mechanism which informs primary user (backuper, respectively) about security incidents of the storage providers providing remote storage space to him. Additionally both of these mechanisms will provide information what are the possible consequences and how to deal with them if possible.

Integration in the demonstrator:

These solutions will be addressed in the form of conceptual specification in the demonstrator.

4.2 Solutions for data minimisation requirements

This section introduces solutions which fulfil requirements on data minimisation introduced in the section 2.2 of this heartbeat. The general goal of the “data minimisation” is to minimise the risk of misuse of the data.

4.2.1 Solutions for data minimisation by anonymisation and pseudonymisation

Section 2.2 of this heartbeat introduces requirements on data minimisation adapted to the privacy-enhanced backup and synchronization demonstrator's environment. Subsection I of the section 2.2 in this heartbeat [H1.3.6, Sec. 2.2, Part I.] talks namely about the need to minimise linkability and observability of the primary user's (backuper's, respectively) actions by using diverse identifiers for different storage providers. This requirement should assure that different storage providers are not able to link his actions or data in case that they would be controlled by a single entity.

Solutions for the demonstrator:

In our demonstrator this requirement will be achieved by generating new credential for each different storage provider and for each different backup (possibly utilizing anonymous credentials). Our demonstrator will also provide functionality for automatic generation of new credentials by using cryptographically secure pseudorandom number generator.

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator.

Subsection I of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part I.] requires additionally, that any delegate should implicitly not be able to link or observe actions of the primary user belonging to different areas of his life or covered by his different partial identities.

Solutions for the demonstrator:

This requirement will be solved by utilizing anonymisation service. Actions of the primary user will therefore stay unlinkable and unobservable among different areas of life or partial identities of the primary user for any authorised delegate. Anonymisation service will assure that the real location of the user cannot be traced by the delegator as well as by storage provider or potential attacker.

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator.

Subsection I of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part I.] requires also, that any potential attacker is not able to observe or link actions of the primary user (backuper, respectively).

Solutions for the demonstrator:

Also this requirement will be solved by utilizing anonymisation service. This will assure, that any attacker observing the communication between primary user (backuper, respectively) will not be able to find out that any two datagrams originated from that particular primary user (backuper, respectively).

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator.

4.2.2 Solutions for minimisation of storage of sensitive data

Subsection II of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part II.] requires, that the storage providers as well as delegates should have only minimal access to personal and sensitive data of the primary user. As far as for the purpose of the demonstrator there is no reason for the

storage provider to access backup data of the primary user the data should be confidential for the storage provider. The same holds for any other third party which is not explicitly authorised by the primary user (delegator, respectively) to access the backup data.

Solutions for the demonstrator:

As far as confidentiality is required, our demonstrator will utilize encryption mechanisms so that confidentiality of the primary user's data is assured. In addition no unauthorised third party, including storage provider, can access the backup data.

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator.

Subsection II of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part II.] applies the minimisation of storage of sensitive data principle also on delegates. Primary user (delegator, respectively) should have possibility to delegate the smallest possible amount of data respecting his areas of life and partial identities sufficient for the specific purpose of the delegation. Primary user (delegator, respectively) should also be implicitly warned that his potentially sensitive data might be irrevocably revealed to selected delegate candidates.

Solutions for the demonstrator:

Confidentiality of the backup data will be solved implicit by data encryption before sending it to the remote storage managed by the storage provider. Delegation of sufficient access rights will be solved by secure access control mechanism. Selection of proper access rights will be under full control of the primary user (delegator, respectively). Primary user's data will be separated according to his different areas of life or partial identities such that distributed storage capacity is effectively utilized. Demonstrator will assist primary user (delegator, respectively) in selection of the proper access condition. When delegating access rights, demonstrator will also provide information about possible risks for that particular type of delegation.

Integration in the demonstrator:

- Encryption of the data before transfer will be fully implemented in the demonstrator.
- Delegation of sufficient access rights by secure access control mechanism will be implemented in such an extent which sufficiently demonstrates this functionality.
- Separation of primary user's data according to different his areas of life or partial identities will be implemented in such an extent which sufficiently demonstrates this functionality.
- Assistance of the demonstrator will be addressed in the form of conceptual specification in the demonstrator possibly with conceptual demonstrative implementation.
- Warning window will be directly implemented in the demonstrator.

4.2.3 Solutions for active support for data minimisation

Subsection III of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part III.] requires, that data minimisation should be actively supported by the demonstrator.

Solutions for the demonstrator: In our demonstrator this requirement will be solved by supporting security mechanisms, which assure unobservability and unlinkability of the primary user's actions as well as anonymisation and pseudonymisation of the primary user's identity.

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator in such an extent, which sufficiently demonstrates this functionality.

4.2.4 Solutions for minimisation of the time frame of data exposition

Subsection IV of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part IV.] requires, that the time frame of the access rights delegated to legitimate delegates should be limited to such a minimal extent, which is sufficient for the purpose of the delegation.

Solutions for the demonstrator:

When delegating access rights, primary user (delegator, respectively) will be implicitly offered delegation valid within limited time frame only according to the purpose of the delegation. Demonstrator will provide the possibility to customize the range of the time frame. The primary user (delegator, respectively) will be warned in case that the time frame selected by user is too extensive according to the purpose of the delegation. He will be asked for explicit confirmation in case of delegating access rights which do not expire at all (with expiration set to infinity).

Integration in the demonstrator:

This solution will be directly implemented in the demonstrator in such an extent, which sufficiently demonstrates this functionality.

4.2.5 Solutions for minimisation of the disclosure of personal data

For the practical solutions of the demonstrator, subsection V of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part V.] is relevant from the primary user's (backuper's or delegator's, respectively) perspective. From this angle, it is required that primary user (delegator or backuper, respectively) should minimise the disclosure of his personal data.

Solutions for the demonstrator:

When delegating access rights to delegate candidates, primary user (delegator, respectively) is warned that as soon as the delegates gain access to his data, the primary user (delegator, respectively) has to rely on the trustworthiness of the delegates because in fact he has no longer direct control on what happens to his data then.

Risk of disclosure of personal data contained in backups will be solved by encryption of the data. Disclosure of personal data resulting from the relationship between storage providers and primary user (backuper, respectively) will be solved by utilizing anonymous (pseudonymous) credentials, anonymous payment system and by generating new identifier for each backup. Also communication between primary user (backuper, respectively) and storage providers will be anonymised. Communication between primary user (delegator, respectively) and delegates will be pseudonymous by default and without the possibility to detect their locations each other.

Integration in the demonstrator:

Utilization of data encryption will be directly implemented in the demonstrator. The further above-mentioned solutions will be addressed in such an extent, which sufficiently demonstrates their functionality.

4.2.6 Solutions for minimisation of the linkability and linkage of personal data

For implementation of the demonstrator, subsection VI of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part VI.] is relevant for the primary user's (backuper's or delegator's, respectively). It is required, that primary user (delegator or backuper, respectively) should minimise the linkability and linkage of his (primary user's, respectively) actions and data, especially among different areas of his life or partial identities.

Solutions for the demonstrator: Linkability of the data and actions of primary user (delegator or backuper, respectively) according to delegates will be avoided by utilizing anonymisation service separating different areas of primary user's life and his partial identities. Linkability of the data potentially collected by storage providers, attackers or other third parties (legally related or not) will be address by integrating anonymisation functionality, anonymous (pseudonymous) credentials and by using generating unique credential for each backup.

Integration in the demonstrator:

Demonstrator will address the above-mentioned solutions in such an extent, which will demonstrate this functionality in sufficient manner.

4.2.7 Solutions for minimisation of multipurpose or context-spanning use of data

Subsection VI of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part VI.] further requires, that the multipurpose or context-spanning use of data should be minimised.

Solutions for the demonstrator:

This requirement will be solved in the demonstrator by utilizing anonymisation service. Moreover, anonymous (pseudonymous) credentials unique for every backup will be used in the demonstrator in order to assure context separation.

Integration in the demonstrator:

Demonstrator will address these solutions in such an extent, which sufficiently demonstrates this functionality.

4.2.8 Solutions for data minimisation by unique identifiers

Subsection VI of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part VI.] also requires, that the data minimisation should be achieved by using unique identifiers which may be used in different contexts.

Solutions for the demonstrator:

This requirement will be solved by generating new identifiers for every backup stored in distributed environment in the storage space provided by storage providers.

Integration in the demonstrator:

The above-mentioned solution will be directly implemented in the demonstrator in such an extent, which demonstrates this functionality in sufficient manner.

4.2.9 Solutions for data minimisation by anonymous or pseudonymous authorisation and access control

Last but not least, subsection VI of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part VI.] requires, that actions between primary user (backuper or delegator) and storage providers or between primary user and delegates as well as delegates and storage providers should be supported by anonymous or pseudonymous authorisation and access control.

Solutions for the demonstrator:

This requirement will be solved by utilizing anonymous or pseudonymous credentials mechanism between all above-mentioned parties.

Integration in the demonstrator:

This solution will be partially implemented in the demonstrator in such an extent, which demonstrates this functionality in sufficient manner. Part of this solution will be addressed in written form as conceptual specification in the demonstrator.

4.2.10 Solutions for data minimisation by minimising irrevocable consequences

Subsection VII of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part VII.] requires, that primary user (delegator, respectively) should always be able to revoke access rights delegated to delegates.

Solutions for the demonstrator:

This requirement will be solved by integrating a mechanism which allows the primary user (delegator, respectively) to revoke his access rights delegated to the corresponding delegates. This action must also generate message to corresponding delegates that their rights have been removed by the delegator.

Integration in the demonstrator:

This solution will be implemented in the demonstrator in such a way, that it sufficiently demonstrates above-mentioned functionality.

Subsection VII of the section 2.2 of this heartbeat [H1.3.6, Sec. 2.2, Part VII.] also requires minimisation of irrevocable consequences requirement in the ability of the primary user (backuper, respectively) to remove any backup item contained in any backup he previously created.

Solutions for the demonstrator:

This requirement will be solved in the demonstrator by implementing a function which allows primary user (backuper, respectively) to delete any backup item and all instances derived from it in whichever backup of the primary user.

Integration in the demonstrator:

Solution of this requirement will be fully implemented in the demonstrator.

4.3 Solutions for privacy-related requirements derived from the backup and synchronization nature of the demonstrator

This section introduces solutions which fulfil privacy-related requirements derived from the specific nature of the demonstrator introduced in Chapter 3 of this heartbeat.

4.3.1 Solutions for localization of the backup data

Section 3.1 of this heartbeat requires that the primary user and the authorised delegates should have a mechanism which allows them to visualize what kind of data is stored in which backup with the possibility to search the data according to selected properties. In addition, there should be a search functionality which allows them to search utilize search request based on several search attributes (see [H1.3.6, Sec. 3.1] for details). On the top of that, all of these actions must be performed in a secure manner so that no attacker is able to reveal what backup item is/was searched, who was searching it or even that it was searched.

Solutions for the demonstrator:

This requirements will be solved by a mechanism which visualizes in which backups (and in how many copies) are particular backup items stored and in what state (e.g., time of last update, older archival version, time of last synchronization). The secure search functionality will utilize anonymisation mechanism in order to avoid linkability and observability. The search functionality will primarily access information about the backup items structure stored locally in order to avoid communication overhead. Information about the structure of the backup items will be stored in special area of each backup. Corresponding secure synchronization of the information about the structure of the backup items will be assured by a special mechanism in anonymous, unlinkable and unobservable way.

Integration in the demonstrator:

These solutions will be implemented in the demonstrator in such an extent, which sufficiently demonstrates the above-mentioned aspects.

4.3.2 Solutions for backup and removal of a single item

Section 3.2 of this heartbeat requires, that the primary user should be able to insert respectively delete any single item to respectively from any of his backups (see [H1.3.6, Sec. 3.2] for details).

Solutions for the demonstrator:

This requirement together with the need to encrypt the data before sending it to the backup (see [H1.3.6, Sec. 4.2.2], [H1.3.6, Sec. 4.2.5]) results into the need to utilize such an encryption schema which allows to insert or remove encrypted data item in a secure manner with respect to further requirements on anonymity, unlinkability and unobservability during the transmission.

Integration in the demonstrator:

A mechanism which fulfils all of the above mentioned properties will be implemented in the demonstrator in such an extent, which sufficiently demonstrates the required functionality.

4.3.3 Solutions for back-in-time recovery

Section 3.3 of this heartbeat requires, that the primary user should be able to use a back-in-time functionality which will allow him to recover not only the most recent version of the backup item created during the last back up action, but also previous versions containing previous state of the corresponding primary item which was backed up in the past (see [H1.3.6, Sec. 3.3] for details).

Solutions for the demonstrator:

A mechanism which provides back-in-time backup and recovery functionality will be provided by the demonstrator.

Integration in the demonstrator:

This solution will be addressed in the form of conceptual specification in the demonstrator.

4.3.4 Solutions for the full deletion

Section 3.4 of this heartbeat requires that the primary user (deleter, respectively) should be able to perform full deletion of any of his backup items (even all backup items), including its copies and older versions, distributed in different backups stored on storages of different storage providers in secure manner supporting revocability of the storage of the data (see [H1.3.6, Sec. 3.3] for details).

Solutions for the demonstrator:

An appropriate mechanism which performs full deletion will be integrated in the demonstrator.

Integration in the demonstrator:

This solution will be addressed in the form of conceptual specification in the demonstrator.

4.3.5 Solutions for backup recovery after unrecoverable crash of the user's system

Section 3.5 of this heartbeat requires, that the primary user should be able to recover all of his backup data (stored in backups) even if he would permanently lost access to his system and data on it (including the demonstrator installed on it).

Solutions for the demonstrator:

This requirement will be solved by implementing a mechanism which will allow the primary user to create secure backup of his credentials used for accessing services of storage providers. This mechanism will allow user to export his credentials to secure media and import them to the demonstrator again in case of system crash.

Integration in the demonstrator:

This solution will be implemented in the demonstrator in such an extent, which sufficiently demonstrates the required functionality.

Chapter 5

Conclusion

In this heartbeat, the concept of the privacy-enhanced backup and synchronization demonstrator selected as the basis for the third year's focal demonstrator is presented. This heartbeat clarifies what the requirements of our demonstrator are. It also outlines the proceeding how they will be fulfilled in the WP 1.3 focal demonstrator. It was presented that the objectives of lifelong privacy lead to practical results, which can be applied for solving real-life issues in enhanced ways. Our demonstrator reveals new problems, which emerge as soon as lifelong aspects related to the data subject are taken into consideration. We presented a new approach, which can help an average citizen to protect himself against unwanted data loss respecting his different partial identities and areas of life. Our approach proceeds in such a way that it takes into account lifelong aspects of a human being and corresponding implications within the scope of the privacy. Furthermore, in this heartbeat we also clarify the reasons, which led us to the decision for selecting the backup and synchronization area as the fundamental base of our further focus.

References

[Böh2009] R. Böhme, M. Raguse, S. Steinbrecher, A. Roosendaal, R. Leenes, H. Buitelaar, A. Kuczerawy, K. Wouters, M. Hansen, I. Scholz, and A. Pfitzmann. Definition of: Prototype ideas for selected scenarios. PrimeLife internal document H1.3.4. PrimeLife - Privacy and Identity Management in Europe for Life, 2009.

[CHPRS2009] S. Clauß, M. Hansen, A. Pfitzmann, M. Raguse, and S. Steinbrecher. Tackling the challenge of lifelong privacy. In eChallenges, October 2009.

[DoW2008] PrimeLife Description of Work. Annex I to the project proposal. (Internal Document), Version 4 as of February 18, 2008.

[Euro1995] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities of 23 November 1995, No L 281, pp. 31-39.

[HPS2008] M. Hansen, A. Pfitzmann, and S. Steinbrecher. Identity management throughout one's whole life. Information Security Technical Report, 13(2):83–94, 2008.

[PBP2009] A. Pfitzmann and K. Borcea-Pfitzmann. Lifelong Privacy: Privacy and Identity Management for Life. In S. Fischer-Hübner, editor, Fifth IFIP International Summer School on Privacy and Identity Management for Life, 2010. Accepted for publication.

[PfHa2009] A. Pfitzmann, M. Hansen: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, December 2009.

[SHR2009] K. Storf, M. Hansen, A. Pfitzmann, S. Steinbrecher, A. Roosendaal, U. Pinsdorf, K. Wouters, A. Kuczerawy, R. Böhme, and S. Berthold. Requirements and concepts for identity management throughout life. Heartbeat H1.3.5. PrimeLife - Privacy and Identity Management in Europe for Life, November 2009.

Appendix A

A. Why we do not go for the existing prototype ideas of H1.3.4

A.1 Criteria for privacy and identity management respecting lifetime aspects

The prototype to be developed shall be able to demonstrate the main concepts and features of privacy and identity management throughout an individual's life. This means that the prototype has to measure up to the theoretical findings in this field. During the previous two years, a couple of articles and reports were published [HPS2008, CHPRS2009, Böh2009, SHR2009, PBP2009], which sketched the problem space of lifetime aspects when managing privacy and identity. In order to serve as reasonable demonstrator of those issues, the prototype is required to exhibit the main characteristics of it. These are described below.

Accordingly, the foremost features the prototype will have to cope with are the different stages of an individual's life, his full lifespan as well as the different areas of life he is acting in as described in [HPS2008]. In this regard, the authors identify mechanisms relevant for

- *user-controlled privacy-enhancing identity management*: handling and management of partial identities, data minimisation, enforceable rules and policies for data processing, and transparency,

in general, and for

- the *areas of an individual's life*: history logging, awareness support, trust and reputation, knowledge and ability to perform typical workflows, interfaces to legacy and emerging systems;
- the *stages of the individual's life*: handling of all delegation-related processes and data, support for different types of delegation as well as
- the *individual's full lifespan*: long-term storage and handling of identity-related data (availability), assurance of long-term robustness of cryptographic protection (confidentiality and integrity),

in particular.

[CHPRS2009] bring dynamics into play, which have a direct implication on "lifelong protection of individuals concerning their privacy in an ICT-based society". They distinguish between

- dynamics in the surroundings of an individual and
- dynamics in an individual's ability and willingness to manage his private sphere on his own.

In the following, when talking about the first category of dynamics we refer to *external dynamics*, whereas *internal dynamics* are referred to when we discuss dynamics of the second category. Those two categories of dynamics have been looked at both from regulatory and technological perspectives in [CHPRS2009].

The main problem regulatory institutions currently have to cope with is that law can only react on detected "consequences of advances in the processing and analysis of personal data". This means that, as privacy-related issues of new technology are not always possible to foresee, threats to privacy will happen before law is set into position to regulate the issues. Nevertheless, the European privacy legislation (Directives 1995/46/EC and 2002/58/EC) state three important legal principles, which data processing has to comply with and which imply data processing over longer periods and spanning different areas of life: 1) the *proportionality principle* – data processing is timely limited to "no longer than is necessary for the purposes for which the data were collected or for which they are further processed" (Art. 6 (1e), Directive 1995/46/EC), 2) the *data minimisation principle* – "minimising the processing of personal data and of using anonymous or pseudonymous data where possible" (Directive 2002/58/EC), and 3) the *purpose binding principle* – personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes" (Art. 6 (1b), Directive 1995/46/EC).

According to [CHPRS2009], technological challenges within the field of lifelong management of privacy and identity mainly comprise robust cryptographic security able to cover an individual's full lifespan as well as assuring potentially required migration of the privacy and identity management system to new hard- and software. Further, the different dimensions of sensitivity of attributes have to be regarded when handling personal data. One of the most challenging concepts that becomes eminent when dealing with different stages of life is delegation. For this, different mechanisms need to be covered, e.g., granting and revoking delegations, accountability as well as transparency of the delegation to the "outside".

A.2 Existing prototype ideas as proposed in PrimeLife Heartbeat H1.3.4

Within the PrimeLife project, several internal deliverables (those are called Heartbeats) were created. They analyzed the different aspects of the given research area and determined requirements to be fulfilled when managing privacy and identity management throughout an individual's whole life. In this course, Heartbeat H1.3.4 specifically collected prototype ideas aiming to implement these aspects [Böh2009].

Due to the huge problem space and given the available resources, it is impossible to design and develop a system that is able to cover the whole problem space of privacy-enhancing identity management throughout individuals' whole lifespan. So, H1.3.4 tried to reduce the complexity of this vast area by structuring it along three general scenarios – Digital Footprint, Growing and Shrinking Autonomy, and Digital Estate – each representing a small part of the problem space. Nevertheless, the scenarios were still quite large and required a lot of interaction between various components and infrastructure to cover them in their entirety. So within each scenario, the scope was further narrowed down to 2 – 3 very concrete prototype ideas. The three scenarios and associated prototype ideas from H1.3.4 are depicted in Table 1.

Scenario	Prototype ideas
Digital Footprint	Show my Digital Footprint
	Remove my Digital Footprint
	Central Data Handling Repository
Growing and Shrinking Autonomy	Passing SNS[2] Sub-Profiles onto Kids
	Assisted Living
	Lifelong DataTrack and Delegation
Digital Estate	Secret Sharing File-System
	Post-mortem Notary Service

Table 1: Scenarios and prototype ideas (cf. H1.3.4 [Böh2009])

A.2.1 Digital Footprint

Three prototype ideas belong to the scenario *Digital Footprint*. One is to give users a tool to gauge the size and shape of their digital footprint (*Show my Digital Footprint*) and to visualize it by different categories. Related to this, *Remove my Digital Footprint* demonstrates an interface to automatically generate rectification or deletion requests for parts of the data in their footprint. Obviously, such reactive mechanisms suffer from weak enforceability, so one step forward could be proactive control of the data handling policies, to which data controllers should obey. The prototype idea *Central Data Handling Repository* helps users to keep an overview of the policies they agreed upon with various services, and assists them in dealing with changes to these policies.

A.2.2 Growing and Shrinking Autonomy

The scenario *Growing and Shrinking Autonomy* covers all aspects where users (temporarily) lack the ability to actively manage their own privacy. In this context, *Passing SNS Sub-Profiles onto Kids* illustrates how parents can control personal information concerning their children in social software and, when the children have grown up, pass it on to them. Similarly, *Assisted Living* shows how visions of computer-assisted care can be realised while retaining as much self-control and privacy as possible for elderly people (or patients). On a more general level, *Lifelong DataTrack and Delegation* demonstrates how various forms of delegation to proxies can be handled in a secure and privacy-respecting manner. The prototype idea focuses particularly on data traces created through delegation. It suggests solutions to the delicate question under which party's control such traces should reside after the delegation relation comes to an end.

A.2.3 Digital Estate

The third scenario, *Digital Estate*, serves as basis for two prototype ideas that show options how to deal with personal information after the death of the respective data subject. *Secret Sharing File System* describes an implementation of Shamir's secret sharing scheme for key recovery. It allows to distribute parts of a master secret (e.g., a password or private key) to a circle of trusted persons, possibly facilitated by making use of social network relations established over social networking

[2] SNS – Social Networking Site

services. In contrast to the grassroots approach, *Post-mortem Notary Service* comes up with a demonstrator for a service that might take over the role of notaries in storing, interpreting, and enforcing a person's testament with respect to his or her digital estate.

A.3 Motivation for the backup and synchronisation demonstrator respecting lifetime aspects and against the existing prototype ideas

Within H1.3.4, a discussion on the suitability of the proposed prototypes for demonstrating the *throughout-life* problem space has been started. For this, the Heartbeat authors refer to related concepts, which were introduced in [DoW2008] and which the prototype should address. Above all, the prototype to be built should contain the mechanisms showing *Long-term aspects of identity formation and evolution*. *History of (partial) identity handling* (Lifelong DataTrack) and *Delegation* are essential concepts for covering the different stages of an individual's life as well as his full lifespan. Related to this are *Policies for long-term access and control* as well as the consideration of *Long-term aspects of sensitivity of identity attributes*. Support of an individual's awareness regarding the processing of his personal data and the related policies – especially with regard to the different areas of his life (*context awareness*) – should also be reflected by the prototype. Further, the prototype is required to offer the possibility to concurrently deal with the dynamics in both the individual's ability or willingness of managing his private sphere on his own (*internal dynamics*) and his outside world (*external dynamics*).

Table 2 summarises how the indicated concepts and proposed prototype ideas fit to each other according to [Böh09]. Those considerations limit the number of possible prototypes as indicated in the following:

→ *Missing important feature(s)*: The first problem that we identified by ranging the prototype ideas in that table is that almost all prototypes (except for *Assisted Living* and *Lifelong DataTrack*) would focus mainly on one area of life only. Thus, their applicability in other *areas of life* is missed though this is one of the major characteristics of the research area and needs to be addressed. The prototypes *Passing SNS Sub-Profiles onto Kids* and *Post-mortem Notary Service* are only singular actions in quite particular *stages of life*[3] and, thus, do not address dynamics in the surroundings of an individual or the individual itself. Similarly, the central concept of *history of identity formation and evolution* is missed within the prototypes *Assisted Living* and *Secret-Sharing File System*.

→ *Existing implementations*: For some of the ideas, either ready[4] or first[5] implementations in form of web-based services already exist. While we should not reinvent the wheel by realising once again the *Show my digital footprint* idea, removing of digital footprints is critical with regard to realisation within the frames of PrimeLife project as it lacks consistent communication structures, technical, and legal concepts. Since establishing these concepts requires a lot of effort to be invested in developing mechanisms that are not focal in the sense of the given research area, it was decided not to go for this idea.

[3] The stages dealt with in these two prototypes are typically at the beginning of adulthood and after death.

[4] *Show my digital footprint* – cf. 123people (http://www.123people.com/) or Kartoo (http://www.kartoo.com/)

[5] *Remove my digital footprint* – "Web 2.0 Suicide Machine" (http://suicidemachine.org/)

	Potential to show dynamics		Concepts for privacy throughout life				
Prototypes	Internal dynamics	External dynamics	Long-term aspects of using sensitive attributes	Policies for long-term access and control	Delegation of identity and authority	Context awareness	History of identity formation and evolution
Show my digital footprint	X	X	X				X
Remove my digital footprint	X	X	X				X
Central Data Handling Repository		X	X	X			
Passing SNS Sub-Profiles onto Kids			X	X	X		X
Lifelong DataTrack and Delegation	X	X	X		X		X
Assisted Living	X		X	X	X	X	
Secret Sharing File System		X	X	X	X		
Post-mortem Notary Service			X	X	X		

Table 2: Prototypes and Concepts (based on [Böh2009)]

→ *Limitation to parts of problem space*: The foremost issue with the introduced prototype ideas is that each of them solves only a particular problem, helps to answer a certain research question, or illustrates how future technology could look like. None of these ideas is actually able to comprehensively cover the concepts of the theoretical framework introduced as key features of lifelong privacy and identity management (cf. Section A.1).

After having drawn these conclusions from the actual prototype ideas, we came to the decision that we need an additional prototype idea trying to cover the majority of concepts, which especially comprises different areas of life, stages of life including the whole lifespan of an individual, and which is able to show dynamics. This led us to the following considerations: In everyday lives, people are interacting with the physical and digital environments. In both of these environments, there are unpredictable events, which we can neither influence nor foresee and which might have an impact on our everyday lives or on lives of our closest relatives. With computerization of society, human beings are not only more and more dependent on the data but they are also becoming data themselves. As far as the influence of the technology on our everyday reality increases, the protection of data and privacy of the corresponding data subject from an increasing number of risk factors is becoming a crucial part of our everyday reality.

Therefore, we decided to design and develop a backup and synchronisation demonstrator specifically respecting and demonstrating privacy and identity management throughout one's whole life. This prototype solves not only the problem of data protection but also the one of protecting privacy of the corresponding individual and, in addition, it respects different areas and stages of the individual's life. Furthermore, our proposed solution deals with the aspect of lifetime and is able to respond to internal as well as to external dynamics.

→ *Comprehensive approach*: The backup and synchronisation demonstrator not only addresses the key features of lifelong privacy and identity management as described in Section A.1. It further incorporates a selection of the main aspects addressed by the previous ideas or it can potentially be enhanced in such a way.

Thus, it will take up issues of *Lifelong DataTrack and Delegation* by allowing for delegation of work items when the primary user is not able to proceed with his work (cf. *stages of life*). A logged *history of data evolution* is required when backup data shall be recovered from a specific point in time. The *Secret Sharing File System* becomes an issue when, e.g., recovery of backup data should only be possible with the help of cooperating participants. The *Post-mortem Notary Service* may become an important instance if backup data should be possible to recover after the primary user has passed away. Similarly, the idea of *Assisted Living* could also be linked to the scenario of synchronising and backing up the states of an elderly person with his nursing service and his medical doctor.