D2.2 Description of Technological Artefacts

Deliverable Number	D2.2
Work Package	WP 2
Version	1.0
Deliverable Lead Organisation	GUF
Dissemination Level	Public
Contractual Date of Delivery (release)	30/11/2017
Date of Delivery	30/11/2017
Status	**Final**

Editor

Jetzabel Serna (GUF)

Contributors

Poornigha Santhana Kumar (USE), Majid Hatamian (GUF), Juan Quintero (UNI), Lamya Abdullah (UNI)

Reviewers

Emiliano De Cristofaro (UCL); Kai Rannenberg (GUF)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

Abstract

This deliverable introduces the design and description of the technological artefacts that aim at increasing individuals' privacy awareness and protection. The objective of these technological artefacts is to transfer the theoretical contributions from the different work packages to practice.
The report presents the technological artefacts developed in the context of the ESR projects 4, 5, 7, and 10. A high-level architecture of the technological artefacts is introduced, followed by the detailed design of components and methods aimed at enhancing usability, transparency, security and privacy in commercial transactions, smartphone ecosystems and cloud services.

Table of Contents

Table of Figures

1 Introduction

One of the major objectives of Privacy&Us is to transfer theoretical contributions from the different work packages to practice by producing different kinds of technological artefacts that aim at increasing individuals' information privacy and as a natural consequence usability and transparency. The main purpose of these technological artefacts is to demonstrate the validity and utility of the developed models and theories that come from different work packages. In this regard, WP2, and more concretely, this deliverable, reports the detailed description of the technological artefacts developed in the context of ESR projects 4, 5, 7 and 10, which address requirements identified in the domains of commercial transactions, smartphone ecosystems and cloud services (D2.1).

In more detail, ESR4's project, a highly secure and privacy-preserving commercial transactions technological artefact, addresses the design challenges in providing secure and enhanced user experience in commercial transactions. In this regard, ESR4 focused on the design and development of an experimental platform for hybrid commercial transactions. A set of methods and tools developed by ESR5, contribute to promote privacy awareness and support informed decision making with regard to privacy. More specifically, the developed artefact aims at increasing smartphone users' privacy awareness through the implementation of privacy indicators and transparency enhancing tools. ESR7's project, contributes to the design of a privacy-preserving Usage-Based Insurance (UBI) system. The design and development of the UBI system is performed according to the value-based IT design principles. ESR10's project proposes a trust-establishment model for privacy-aware Cloud services. This model addresses the privacy and confidentiality requirements and challenges in smart environment applications. The proposed model allow for an early evaluation with regard different aspects and theories of trust-establishment in smart environments, as well as in cloud services.
Following this report, the final report of WP2 (D2.3, month 44) will provide details about the validity and utility of the individual technological artefacts introduced in this deliverable.
In the development of this deliverable, ESRs 4, 5, 7 and 10 also contributed by actively providing feedback to other projects and finding potential synergies for joint collaborations.
Opposite to the initial plan, ESR Projects 9, 11 and 13 are not included in this deliverable, the rationale behind this decision is detailed in the following.

ESR 9 (TAU) is no longer included in WP2 as initially planned because in order to best contribute to her career development and to allow the project to best utilize her skills, ESR 9 will not develop a technological artefact. The revised project (Reframing Informed Consent in Information Privacy Law Through Behavioural Economics and the Paternalism-Libertarianism Spectrum) will instead use legal theory, concepts from behavioural economics and political economy, and comparative analysis with other fields, to analyse shortcomings in the validity and effectivity of the informed consent requirement in American and European Law, and explore suitable tools available to remedy or mitigate those shortcomings.

ESR 11 (UCL) is not included in this deliverable. The research plan of ESR11 considers developing an artefact but only during the second stage of his PhD. Based on an extensive review of the genomic privacy work, with the form of a Systematization of Knowledge paper[1], several gaps and challenges in the state-of-the-art work have been identified by means of a systematic research methodology. However, before an artefact can be implemented to address one or more of said gaps, the ESR must conduct work to provide a user-centred view on the problem. This will be informed by user studies designed and conducted during his secondment at Bonn. The results of this research are expected during the spring of 2018, and thus, the development of the artefact can begin only after that.

ESR 13 (VDS) is not included in this deliverable. The research plan of ESR13 does no longer consider developing an artefact. Based on an initial literature review, several knowledge gaps on the state-of-the-art technology (i.e. online banking) have been identified. Before an artefact could have been developed, these knowledge gaps should be addressed, which ESR13 is planning to do. Due to the expected effort for this, the development of an artefact afterwards is unlikely.
The current project plan is as follows (see D1.4): Through a set of qualitative user studies, this research aims to evaluate the state-of-the-art in transaction authentication: online banking. An initial

[1] https://www.ieee-security.org/TC/SP2018/cfpapers.html

literature review revealed several knowledge gaps, related to user's mental models of transaction authentication, economic and technical constrains on the design of artefacts, and the effectiveness of state-of-the-art technology. Qualitative user studies will consider a wide set of methodologies, such as participant observation, interview, focus group, card sorting, drawing, co-design workshop, role playing, prototyping, cognitive walkthrough, retrospective walkthrough, journey maps, personality assessment scales, and others. Appropriate methods for analysis of the data will be chosen based on each study's individual design. Based on the insights gained, this project will then continue to design mitigation approaches for identified adverse factors, propose advancements to the state-of-the-art technologies, or further investigate requirements of specific user groups.

2 Technological artefacts

This chapter introduces the theoretical research results in the form of detailed designs of technological artefacts developed in the context of the ESR 4, 5, 7 and 10 projects. The design of the introduced artefacts, follow the Agile process[2], as a continuation of the methodology already adopted in the requirements analysis.

2.1 ESR4 (USE) Designing for Privacy & Security at Point of Sale Commercial Transactions

Technological artefact: A model for designing secure experiences in hybrid-commercial transactions
ESR: 4 – Poornigha Santhana Kumar (USE)

The technological artefact consists of a platform for conducting experiments on hybrid commercial transactions. The platform offers a number of prototypes, each of them consisting of a payment terminal and NFC mobile device aimed at assisting security system designers, in the development and validation of best practice models for designing scalable, robust and secure interfaces and services for hybrid commercial transactions. As a result, this artefact will lead to a commercially viable secure hybrid-experience prototype.

2.1.1 High level architecture model

The platform allows for the development of various high fidelity prototypes (working prototype) for hybrid commercial transactions using NFC. Figure 1 depicts the basic commercial transactions architecture, which is the basis of each prototype.

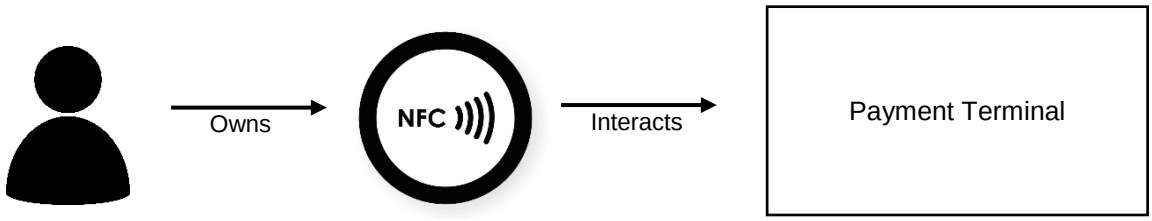

Figure 1 Commercial transaction architecture

As shown in Figure 1. Each prototype consists of two components. The NFC component and the payment terminal. The user interacts with the payment terminal using an NFC component.

[2] Kent Beck, James Grenning, Robert C. Martin, Mike Beedle, Jim Highsmith, Steve Mellor, Arie van Bennekum, Andrew Hunt, Ken Schwaber, Alistair Cockburn, Ron Jeffries, Jeff Sutherland, Ward Cunningham, Jon Kern, Dave Thomas, Martin Fowler, Brian Marick (2001). "Manifesto for Agile Software Development". Agile Alliance.

For the development of the platform, in this project we limited the scope to those NFC component types used in Austria. Thus, the user may own any one form of NFC introduced next.

- NFC card
- NFC sticker
- Mobile NFC (mobile application)

Similarly, we limited the scope of this project to the various types of payment terminals used in Austrian supermarkets. More concretely, the following types of payment terminals are used in the prototypes

- Terminal with no feedback
- Terminal with audio feedback and no visual feedback
- Terminal with both audio and visual feedback

As a result, each developed prototype keeps the same basic architecture (Figure 1) whereas the main components used are altered. The main goal, is to identify the most suitable combination of NFC component and payment terminal that provides the user with secured and privacy enhanced experience. The resultant prototype - NFC component and terminal, will then be used as the basis for the design of the final commercial transaction.

2.1.2 Detailed design and modelling

This section introduces the detailed design and modelling of the components used in the prototypes.

2.1.2.1 The NFC component

In what follows, the detailed designed of each component is sketched.

Component name: NFC enabled traditional debit card

Description: Traditional debit card with NFC functionality

Requirement(s) addressed: Easy to use.
No training/adaptation needed from user

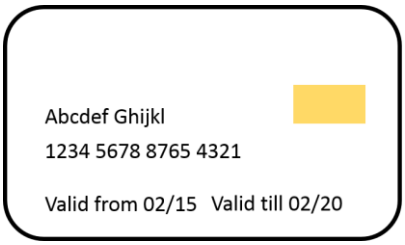

Figure 2 NFC enabled debit card

Component name: NFC enabled *debit* card minimum details

Description: *debit* card with only expiry date and NFC functionality

Requirement(s) addressed: Very less loss of information in case theft

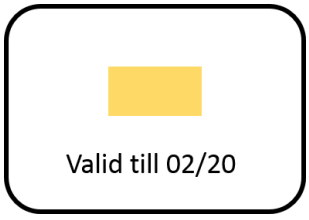

Figure 3 NFC enabled debit card with minimal information

Component name: NFC Sticker

Description: Sticker attachable to users' belongings like watch, mobile phone etc.

Requirement (s) addressed: Easy to use. Reduces risk of theft or being lost

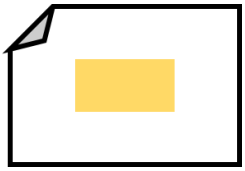

Figure 4 NFC sticker

Name: (bank) Mobile NFC

Description: Mobile application provided by bank that replaces NFC card. It allows users to make payments and manage NFC transactions

Requirement (s) addressed: Provide feedback about the transaction to the user. Easy access to NFC transactions

Figure 5 Mobile NFC

Name: (third party) Mobile NFC

Description: Mobile application provided by third party that replaces NFC card. It allows users to make payments and manage NFC transactions

Requirement (s) addressed: Provide feedback about the transaction to the user. Easy access to NFC transactions

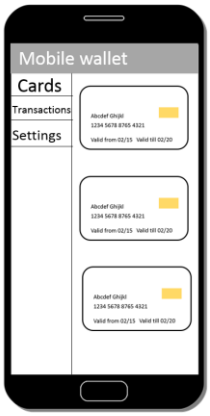

Figure 6 Third-party mobile NFC

2.1.2.2 **The payment terminal**

In this subsection the detailed designs of the payment terminal components are introduced.

Component name: Terminal with (screen) NFC symbol

Description: Payment terminal with marking on where to scan the NFC component on the screen

Requirement(s) addressed: Clearly state users how to initiate a transaction

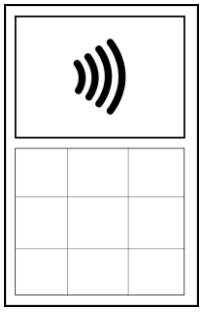

Figure 7 NFC terminal with NFC symbol

Component name: Terminal with (hardware) NFC symbol

Description: Payment terminal with marking on where to scan the NFC component on the terminal hardware

Requirement(s) addressed: Clearly state users how to initiate a transaction

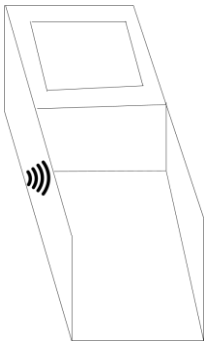

Figure 8 NFC terminal with NFC symbol on hardware

Component name: Terminal with clear (screen) visual feedback

Description: Payment terminal with visual feedback on screen

Requirement(s) addressed: Deliver user with information on the state of transaction. Notifies users when the transaction is complete

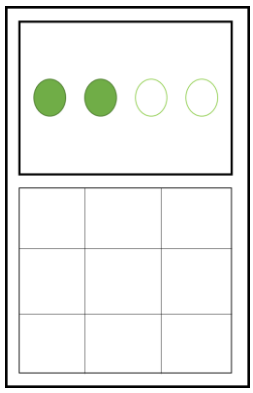

Figure 9 Terminal with feedback on the screen

Component name: Terminal with clear (hardware) visual feedback

Description: Payment terminal with visual feedback on the terminal hardware

Requirement(s) addressed: Deliver user with information on the state of transaction. Notifies users when the transaction is complete

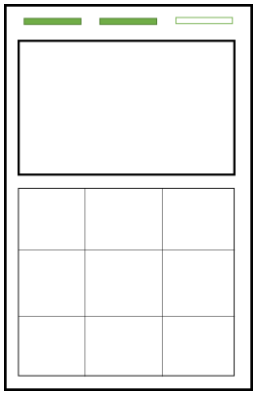

Figure 10 Terminal with feedback on the hardware

Component name: Terminal with clear audio (during transaction) feedback

Description: Payment terminal with multiple short beeps during the transaction and one long beep at the end of transaction

Requirement(s) addressed: Deliver user with information on the state of transaction. Notifies users when the transaction is complete

Component name: Terminal with clear audio (beginning transaction) feedback

Description: Payment terminal with one beep at the beginning and end of transaction

Requirement(s) addressed: Deliver user with information on the state of transaction. Notifies users when the transaction is complete

2.2 ESR5 (GUF) Privacy Indicators in Smartphone Ecosystems

Technological artefact: An instrument to collect and display privacy experience reports in smartphone app ecosystems
ESR: 5 – Majid Hatamian (GUF)

The technological artefact is aimed at increasing the smartphone users' awareness of privacy. This is achieved by implementing and developing mechanisms that support users to make informed decisions. These mechanisms are ultimately integrated to provide a concrete smartphone app that helps and supports users to preserve their privacy.

The proposed technological artefact follows two main goals:

1) Providing transparency for smartphone apps: through a transparency tool that inform users in a user-friendly form about the privacy related behaviour of their installed apps, e.g., resource accessed, frequency, etc.

2) Providing a comparison of apps regarding privacy: through a method that uses user reviews on app stores in order to classify them and extract knowledge based on the facts stated in the users' claims. Results from this method enabled the implementation of a privacy scoring system that calculates the privacy sensitiveness level of apps by analysing user privacy reports.

2.2.1 High-level architecture model

Figure 11 shows a high-level overview of the proposed artefact. The artefact consists of two main components, including the Android App Behaviour Analyser (A3) and the privacy risk analysis component based on user reviews.

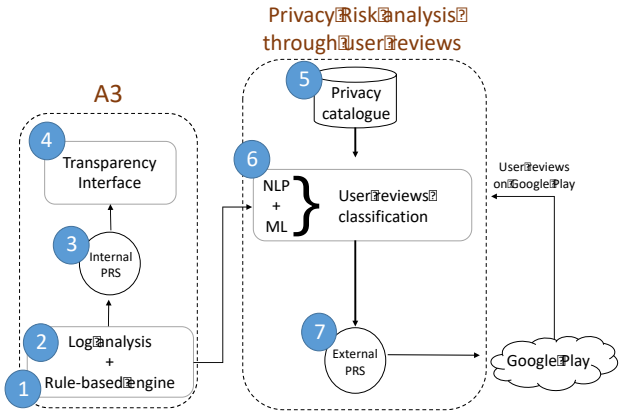

Figure 11 High level architecture of the android app analyser

The proposed artefact comprises two main components. These components are jointly working together.

2.2.1.1 Android App Behaviour Analyser (A3)

This component is responsible to monitor the installed apps on the smartphone. A rule-based engine will be initiated to extract any privacy deviated behaviour from the apps. The results obtained from the combination of these two concepts (log analysis and rule-based engine) will further be communicated

to the user through a graphical user interface as a form of a detailed view of resource accesses and a privacy risk score.

2.2.1.2 Privacy Risk Analysis through User Reviews

This component is responsible to measure the privacy risk score. The risk score is calculated based on knowledge extracted from user reviews on app stores. The component requires the employment of machine learning techniques in order to classify user reviews into different privacy classes to differentiate apps with the worst privacy protection issues. It is worth to mention that this component implemented on the user's device but rather at the server side, following a server client architecture.

2.2.2 Detailed design modelling

This section introduces a more detailed description of individual components and methods used in the technological artefact.

2.2.2.1 A3: methods and components

This section includes the descriptions regarding the design of log reader, rule-based engine, internal privacy risk score (PRS), and transparency interface.

Log Analysis: This component analyses the behaviour of installed apps on users' device. We first implemented a log reader based on AppOps, which is a privacy manager tool and introduced in Android 4.3. In order to collect the logs, a timer is sent to the *PermissionUsageLogger* service periodically. When it is received, the logger queries the AppOps service that is already running on the phone for a list of apps that have used any of the operations we are interested in tracking. We then check through that list and for any app that has used an operation more recently than we have checked, we store the time at which that operation was used in our own internal log. These timestamps can then be counted to get a usage count. It is worth to mention that the log analysis will happen in the user's device.

Rule-based Engine: This component identifies privacy deviated behaviours. It receives as an input the results from the log reader, and analyses them in order to detect anomalous behaviours. It is based on predefined rules that can be dynamically updated providing advanced functionality and high flexibility. An example of these rules can be seen in Figure 12.

```
1 #When the display is off and critical resource was used, but
      without the case of taking a phone call
2 if((criticalRecources.contains(resource)) && (screenState ==
      0) && !(closeToObject == 0) && !(resource.equals("
      RECORD_AUDIO"))){
3     results.add("1");
4     results.add("Screen was off and critical Resource was used
      ");
5     return results;
6 }
```

Figure 12 Rule-based engine: example rule

Local Privacy Risk Score: It represents a privacy metric to inform users about the privacy invasiveness level of monitored apps and it is calculated as the ratio of privacy sensitive permission accesses in time *t*, meaning that:

$$\frac{number\ of\ privacy\ sensitive\ permission\ accesses}{total\ number\ of\ permission\ accesses}$$

The results of such calculation are then communicated to the user through a transparency interface.

Transparency Interface: A3 is aimed to appropriately inform the users of the potential misuses of their personal data. We believe an appropriate and efficient GUI should be able to raise the awareness of misconduct of apps. For this reason, the Graphical User Interface (GUI) plays a crucial role in A3. We display a summary of apps and resources accessed including the corresponding timestamps. To increase the usability aspects, we mapped/translated the permissions from those defined by Android to a common language definition. Finally, to encourage users to take actions when potential privacy risks were detected, our component provided the interfaces to either restrict a permission or to report a resource. Figure 13 shows the user interfaces in a more detailed form. This component addresses the requirement of showing privacy risk score to the user,

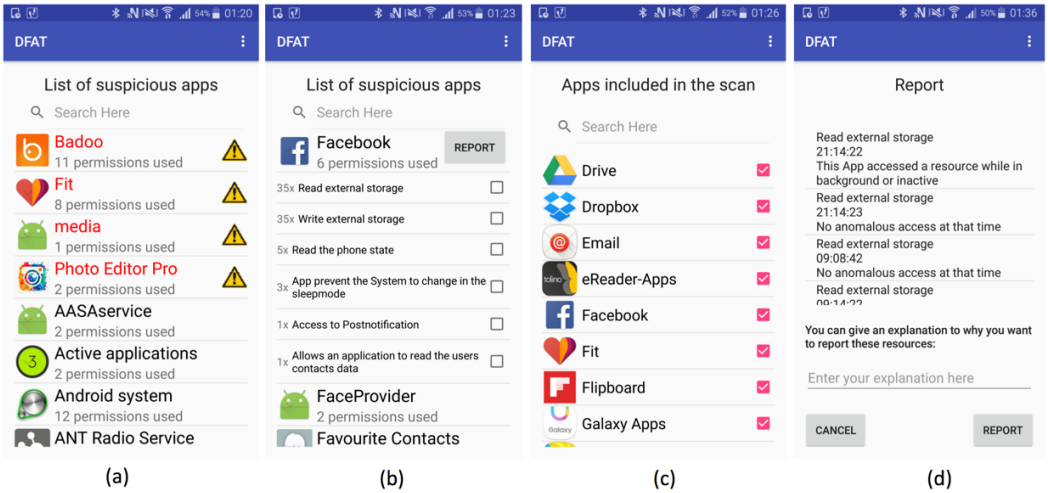

Figure 13 Different screens of A3, (a) list of scanned apps, (b) details of accesses, (c) selectively choosing apps that need to be scanned, and (d) descriptions of resource accesses.

2.2.2.2 Methods for Privacy Risk Analysis

In this section we introduce the privacy risk analysis component, which, goal is to measure the privacy risk level of a given app when compared to other similar-functionality apps. To achieve this, user reviews on Google Play are used and processed by exploiting machine-learning techniques.

Privacy Catalogue. The aim of the keyword catalogue is to support the labelling/classification task; that is, for each new user review, one or more privacy labels were assigned. To this end, we developed a keyword catalogue based on i) the privacy-relevant Android permissions set; ii) the insights gained from the preceding literature review.

User Reviews Classification. In order to classify user comments, we employ supervised machine learning methods applied on natural language processing (e.g. SVM). As this component is used as the input for the external PRS, each user review is classified according to none, one, or more labels. We use SVM as our classification technique, in which each data point is shown in a feature space. In our case, the features represent words, which appear in the user reviews. The development phase of our classifiers included training and testing. The training phase is the step where the classifier is determined and optimised. After the classifiers are trained, performance checks are undertaken to compare how the class output of the algorithm compares to the labels given by the user.

External Privacy Risk Score. This score is calculated based on users perception regarding to privacy issues detected in apps. To quantify this, we used the ratio between the number of privacy-related comments of an app to a category-specific number of comments. This category-specific indicator represents the number of privacy-related comments found in all applications from a certain category.

In the following, we describe how different components of the technological artefact address the functional requirements elicited in D2.1.

Component name: Log analyser
Description: scans the device for resource accessed by the installed apps
Requirement(s) addressed: Smartphone scanning

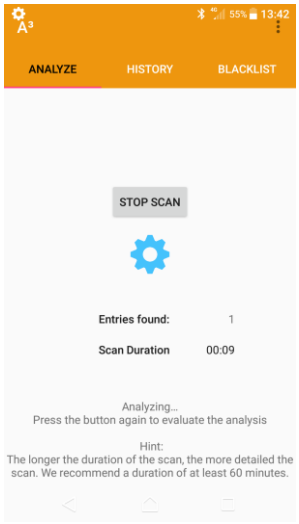

Figure 14 Log analyser

Component name: Log analyser and transparency interface
Description: Allows users to manage the log history, store, search and delete
Requirement(s) addressed: *Log History*

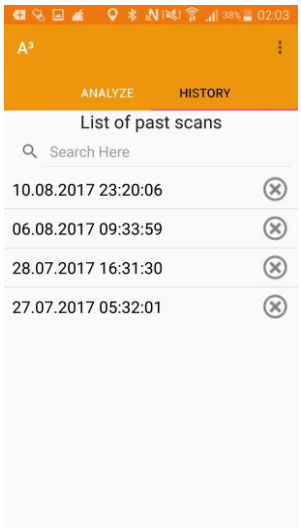

Figure 15 Log analyser results on transparency interface

Component name: Transparency interface
Description: Informs the users about apps behaviour and redirects the user to the Android Permission Manager
Requirement(s) addressed: *Permission granting*
Users are encouraged to decide which permissions they do not feel comfortable to still grant to a certain app by redirecting them to Android Permission Manager

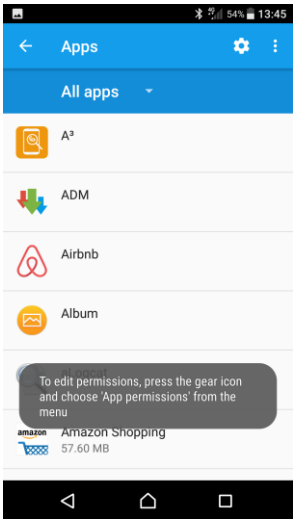

Figure 16 Transparency interface

Component name: Privacy risk score components (local & external)
Description: The privacy risk score components (both internal and external) are responsible to provide user with a metric that is aimed to increase the user's awareness of privacy.
Requirement(s) addressed: *Privacy Risk Score*

Component name: Transparency interface – feedback module
Description: Allows the user to report privacy invasive behaviours of apps.
Requirement(s) addressed: Network Connection
Although the proposed artefact does not send any information to external servers by default and the main processes are performed locally (on the user's device); the mechanism to send feedback regarding the privacy invasive activities requires network connection. Thus, users have the possibility to switch between Wi-Fi and network (and vice versa) connections when one of them is not accessible

Component name: Rule based-engine
Description: Identifies anomalous behaviours based on pre-defined rules
Requirement(s) addressed: Extensibility
The design of the component allows for more rules to be added in order to provide more fine-grained privacy deviated behaviour detection.

Component name: Log analyser
Description: Scans installed apps resource requests
Requirement(s) addressed: OS Modification/Device Rooting Avoidance
By accessing to the AppOps logs, there is no need to root the device, as they are accessible to any app with debugging privileges.

2.3 ESR7 (UNI) The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications

Technological artefact: A Usage-Based Insurance (UBI) system designed according to the value-based IT design principles
ESR: 7 – Juan Quintero (UNI)

Usage-Based Insurance(UBI) is a technical term referring to an auto insurance system that "enables insurance companies to collect individual consumer's driving data and provide individually targeted price discounts based on each consumer's driving behaviour" [2]. UBI is an instance of Usage-Based Pricing (UBP) which is defined in [2] as "system that sets prices based on consumer's usage of a product". The consumer's driving data can be used by insurance companies not only to set personalized prices, but also to reduce their incurred losses using more accurate risk estimations [1]. UBI encourages the drivers to practice safe driving and limit vehicle usage, reducing fuel consumption and contributing to have a cleaner environment. The chance of an accident can be reduced, resulting in enhanced safety levels of citizens [6]. UBI advantages are presented in **Error! Reference source not found.**.

Advantage				
	Consumer	Environment	Insurers	Society
Provide a real-time feedback to consumers	+	+	+	+
Implement a call emergency services	+		+	+
Fight against fraud	-		+	+
Fight against vehicle theft	+		+	+
Apply a pricing based on risk profile	+/-		+	+
Reduce accidents	+	+	+	+
Reduce claim cost	+		+	
Reduce CO_2 emissions, fuel consumption, loss of live, and road congestion	+	+		+

Table 1. Advantages to implement UBI programs [2, 4, 5, 6]

However, UBI also has some disadvantages [4]:

1) Consumer's privacy: Insurance company and other involved parties (partners) could use the consumer´s data for other purposes different to pricing and improving consumer´s driving style, for example to track the user position, attend claim settlements, or fight against frauds.
2) Discrimination: Most current UBI programs are designed for small group, such as young people, newbie driver (little driving experience), and family with a young member.
3) Transparency: The insurance policy holder is not aware of which data are collected and how these data is processed, stored, and shared by the insurance and third-parties. In many cases, a UBI program may look like a black box approach to get a consumer rating and information.

The technological artefact is a UBI system designed according to the principles of value-based IT design [3].

2.3.1 High level architecture model

Figure 17 depicts a UBI canonical model, showing how a User (policyholder) provides his or her driving data to insurance company to calculate a premium and get a feedback based on his or her driving style.

The collected data can be, depending on the UBI program: driving time, location, speeding, acceleration, braking, steering, and direction and distance travelled. Some of this data can be directly collected using various sensors, other data types can be calculated from the collected data, depending

on the telematics device. This huge amount of data (personal identifiable (PI) and non-PII) should be stored, accessed, and processed according to the data privacy regulations.

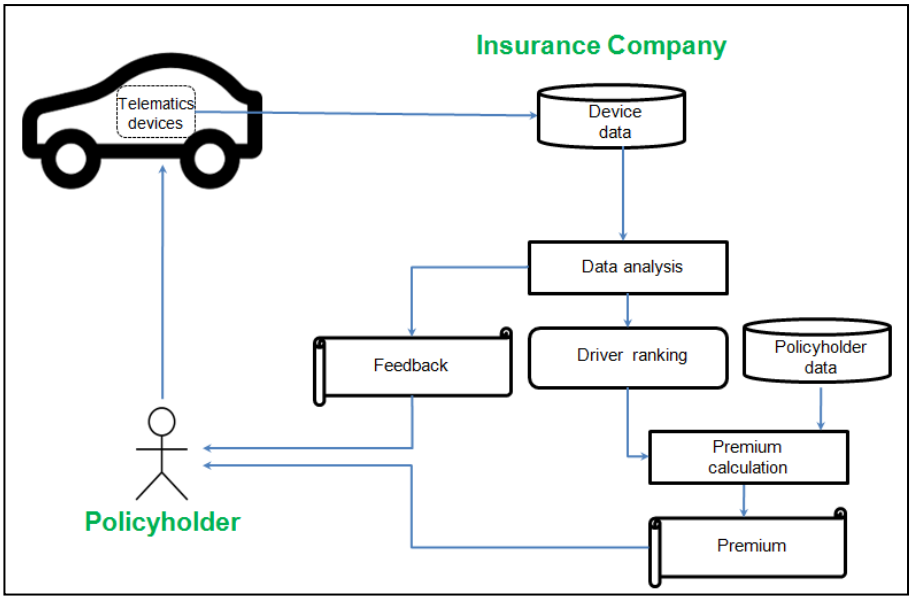

Figure 17. UBI canonical model

In Figure 17, components such as Device data, Data analysis, Driver ranking, and Feedback can be identified as high privacy invasive, owing to driving data with PII would be using. Therefore, the contribution is to design a UBI system that supports human values, such as privacy, control, transparency, trust, safety, integrity, and confidentiality, using Friedman´s methodological framework (Figure 19). In the green square in Figure 18 is lighted the most privacy invasive process in a UBI system. I will focus on these components. The User can access and see his or her data and get feedback about his or her driving style through an interface (Smartphone app or website).

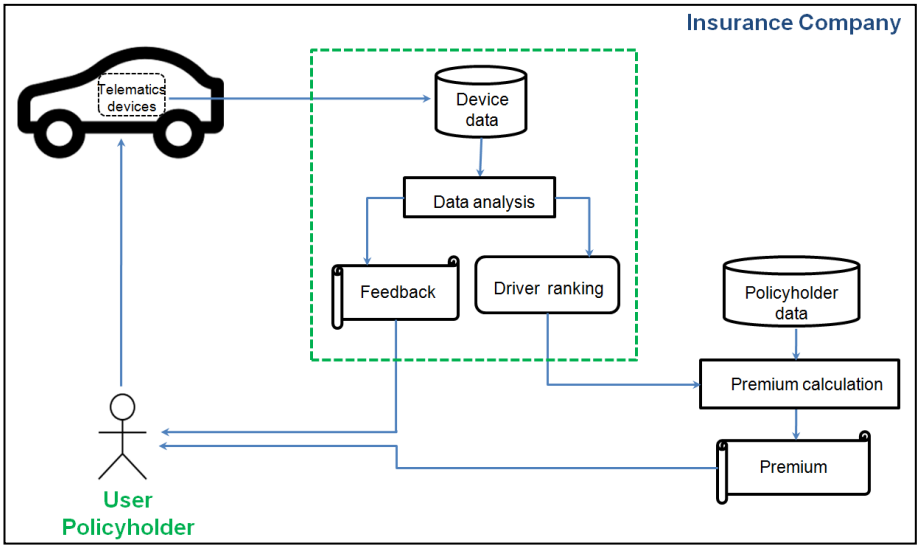

Figure 18. First approach to the technological artefact

Next subsection describes Friedman´s methodological framework.

2.3.1.1 Value-based IT design (VBD)

Friedman et al, [7] described a methodological framework to design based on values, which is called value-sensitive design depicted in Figure 19. First, a **conceptual investigation** (value discovery and value conceptualization) is conducted in order to identify the Stakeholders (direct and indirect) in our

system. Willcoks and Mason [8] define Stakeholders as “people who will be affected in a significant way by, or have material interests in the nature and running of the new computerized system”. VBD considers 2 different Stakeholders, defining in [7] as:

- Direct. Parties, who interact directly with the system or its output
- Indirect. Other parties affected by the use of the system without interact directly with the system

The conceptual investigation is a phase where the direct and indirect Stakeholders are identified. In the Empirical investigation phase, different empirical methods can be used to address the questions about projection of technology and stakeholders affected. Finally, technical investigation is focused on how nature can be embedded in the design of the projection technology, using the result obtained in conceptual and empirical investigation phases. In this point, all architecture’s details will be defined.

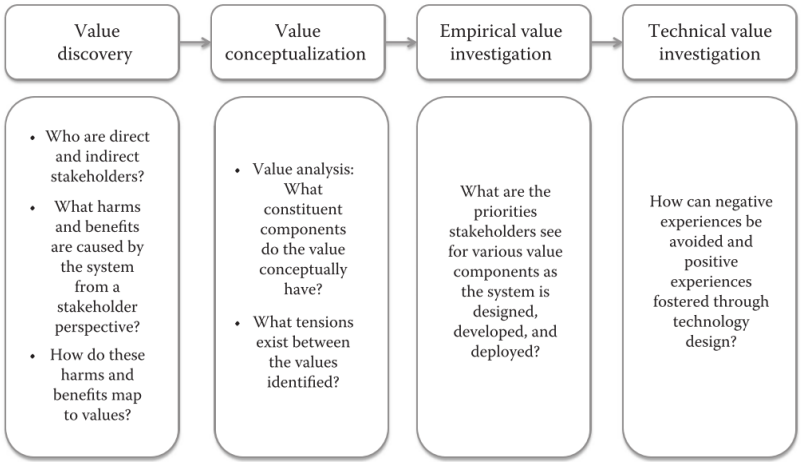

Figure 19. Friedman’s methodological framework [3, p.168]

My contribution in this work package is contained in the ***Technical value investigation*** phase. The previous phases are being worked in the work package 3 (Model of behaviour).

2.3.2 Detailed design modelling

To design a system using the principles of value-based IT design, in the Figure 20 a roadmap is drawn.

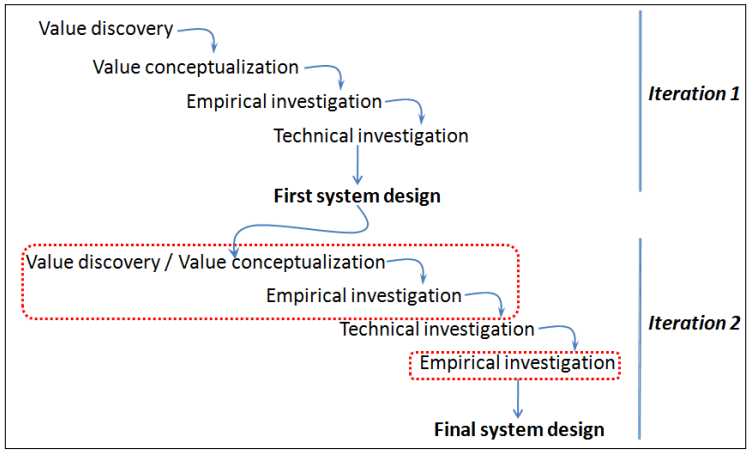

Figure 20. Roadmap of value-sensitive design framework

The design will be performed in an incremental and iterative process, executing two iterations to reach a final system design. A Value discovery, Value conceptualization, Empirical investigation, and Technical investigation phases are performed in the iteration one to reach a first system design, which

will be the input to the iteration 2. During the iterations, the system design is refined, based on the user study feedback and the value integration in the design.

The iteration 2 includes two empirical phases to validate and refine the system design. In this iteration a Value discovery and Value conceptualization are carried out to identify additional values from the first system design. Also, an empirical investigation phase is used to validate the first iteration output, conducting a user study. Then a technical investigation and an empirical investigation are performed, putting up a final system design.

The core of this work package is the technical investigation phase, where two tasks (analysis of existing UBI solutions and study sealed computation) are executed in parallel before to conducting an analysis of existing UBI considering Values. After that a solution will be designed according to the principles of value-based IT design.

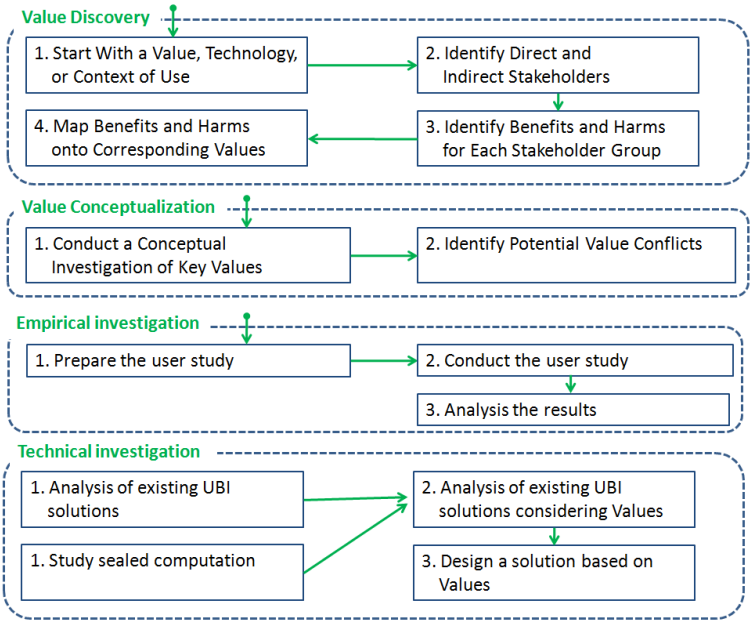

Figure 21. Value-sensitive design phases

The approach to a system designed according to the principles of value-based IT design will be validated in the iteration two into the Value discovery, Value conceptualization, and Empirical investigation using the iteration one feedback and the first system design. These validations are represented in red square in the Figure 20.

The phases: Value discovery, Value conceptualization, and Empirical investigation belong to work package 3 (Model of behaviour). Currently the iteration one is running and two initial tasks of Technical investigation (analysis of existing UBI solutions and study sealed computation) are being performed. In the task “analysis of existing UBI solutions considering Values” in Technical investigation phase will be written user stories based on the information gathered in the previous phases, focusing on the user story “Bonus in car insurance” described in the deliverable 2.1 (D2.1) in the section 2.3.1.2. The other epics user stories described in D2.1 in the ESR07 project will not be taking into account; due to this project has been focused on the Usage-Based Insurance scenario.

In 2.3.2.1 is described a high level user stories proposed at this early stage.

2.3.2.1 User stories

2.3.2.1.1. Bonus in car insurance

Story Narrative	Bonus in car insurance	*Priority*	*must*
As a	Insurance company	*Size*	*epic*
I want	to analyze the Policyholder data to find out behavior patterns (driving style, speed, etc.)		
So that	Policyholder gets a reward with new offers or discounts in his car insurance		

[front of card]

Acceptance Criteria	Bonus in car insurance
Given	Policyholder with a contracted car insurance
When	A good driving style is obtained from the Data Subject data
Then	Policyholder receives a notification with the reward

[Back of card]

2.3.2.1.2. Feedback on driving style

Story Narrative	Feedback on driving style	*Priority*	should
As a	Policyholder	*Size*	theme
I want	to get feedback on my driving style		
So that	I can improve my driving style and get a discount on my insurance policy		

front of card

Acceptance Criteria	Feedback on driving style
Given	A way to see the feedback
When	Policyholder uses this way
Then	He/She will be informed about the feedback on his/her driving style, including historical information

Back of card

2.3.2.1.3 Store device data

Story Narrative	Store device data	*Priority*	must
As a	Insurance company	*Size*	theme
I want	to store the device data, which contain policyholder driving data		
So that	I will be able to have data to calculate an individual risk and offer a discount to the policyholder		

front of card

Acceptance Criteria	Store device data
Given	A repository with the device data collected
When	the insurance company accesses the device data
Then	the device data will be available

Back of card

2.3.2.1.4 Calculate drive ranking

Story Narrative	Calculate drive ranking	*Priority*	must
As a	Insurance company	*Size*	theme
I want	to calculate an individual drive ranking		
So that	the policyholder will get a discount and I will have an individual risk estimation		

front of card

Acceptance Criteria	Calculate drive ranking
Given	a repository with the device data collected
When	an analysis process will be performed
Then	insurance company will get a drive ranking

Back of card

2.4 ESR10 (UNI) Adaptive Data Privacy for Smart Environments

Technological artefact: A trust establishment model for privacy-aware cloud services
ESR: 10 – Lamya Abdullah (UNI)

2.4.1 High level architecture model

The artefact consists of a privacy-aware model to establish trust in cloud computing that relies on a technological base combined with a non-technological base that reduces the subjective trust on the cloud providers. The model covers the main two stages of trust management – trust establishment and trust maintenance. The purpose is to enable cloud clients including the users of smart environment applications to ensure the confidentiality and privacy of their data stored in the cloud. The model structure is based on the general architecture of cloud-based applications.

The model aims to manage trust among participants to eliminate the need to trust only one participant in the system so that no single party can compromise the properties of the system. The main roles of participants in an abstract cloud-based application we used are summarized as below:

- **Data producers (user):** produces and provides data.
- **Data Consumers (user):** consumes the results computed by the analytics software provided by the ASP.
- **Application Software Provider (ASP):** develop the analytics software to be run on the stored data in the cloud servers.
- **Cloud Provider (CP):** provides the cloud service that includes the infrastructure, visualization, platforms, configuration and deployment environment and security of the system as well as availability.
- **Auditor:** guarantees the integrity of the system

The model relies on the notion of sealed computation and on the role of the auditor providing a mechanism of remote attestation. Figure 22 below, describes the abstract structure of the model. The details of trust establishment and trust maintenance in the model are described in the illustrated in the next section.

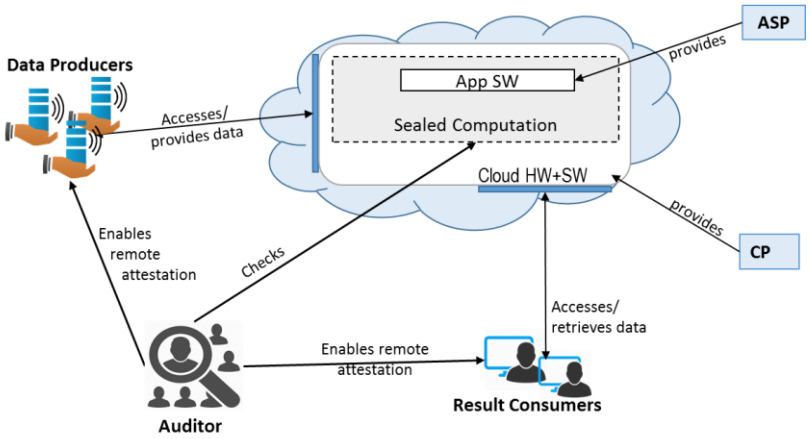

Figure 22: Trust model structure

Participants' general requirements:
In the proposed general model, we assume the following requirements set to be fulfilled for participants in smart applications using cloud computing:

- Data Privacy and confidentiality apart from results that the consumer is supposed to get.
- Service availability: if data producers want to feed data into the system, the system shall receive it, similarly, the service needs to be available to provide results when needed.
- Results integrity: results are correctly computed on data as provided by data producer
- Software integrity and confidentiality: the developed software is executed unmodified and is not exposed to anybody apart from CP and Auditor.
- Confidentiality of the attestation credential: so that the credential don't leak out of the system.

2.4.2 Detailed design modelling

We represent the model as steps and interactions between different participants during trust establishment in a UML alike diagram, Figure 23.

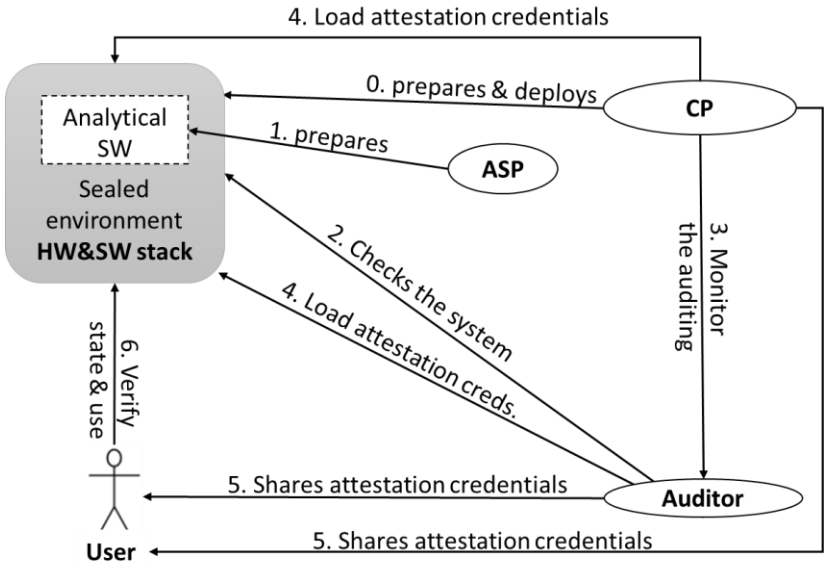

Figure 23: Trust establishment model - UML

The main steps are:

- The cloud provider prepares the system including the sealed computation mechanism, and the ASP prepares the application software. The application is deployed, and system is ready for check.
- The auditor checks (off-line) the integrity of the sealed computation system – both the HW and SW - that includes a physical check for the security measures, policy compliance, data security and data privacy, functional check, etc.
- CP ensures that the auditor is behaving according to the auditing procedure specifications
- Both, the auditor and the cloud provider, generate their attestation keys (private keys) and deposit them to the system. [the end of auditing procedure].
- The system then is ready and shipped to the cloud centre if not there already (complete system with the infrastructure) and the service is up and running.

- Both CP and the Auditor distribute the corresponding attestation keys (public keys) for application users, such as the data producers and data consumers in addition to administrators such as the application service provider.
- Data producer and/or data consumer use the public key of both the CP and the Auditor as the credentials to verify the state of the system (cloud).
- Auditors must be present any time when the system and/or the sealed computation mechanism is restarted or under maintenance and changed and shall re-check the system and both (the Auditor and the CP) re-reload their attestation keys.

Trust maintaining is achieved in a distributed manner during the lifetime of the system, the below figure shows the timeline of trust management as held by each party in the model.

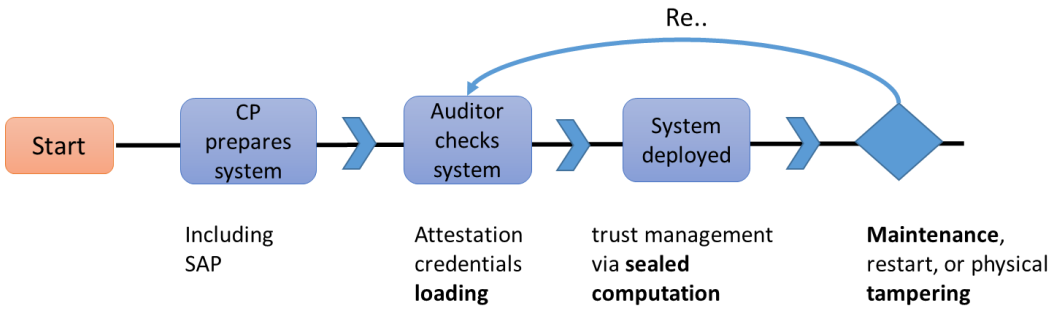

Figure 24: Trust management during the system lifetime

The proposed the model considers the requirements as described briefly in D2.1 Requirements Analysis.

- Data secrecy: privacy of the user data from the provider is ensured by the usage of the sealed computation.
- Data privacy transparency: the model utilizes the role of an auditor which can be extended further to communicate the system state with the user to ensure that the minimum requirements are fulfilled as agreed.
- Data Availability: it is assumed in the model that the data producer is required to provide data and to be made available so that the application is running. Intuitively, it is out of scope of the current model since there must be needed data for the application as agreed by the specification.
- Intervenability: The model at this stage focuses on privacy from the infrastructure provider and operator so that it does not consider user changes for how data is processed.

3 Conclusions

The technological artefacts developed by ESRs 4, 5, 7, and 10 follow the Agile methodology and are presented as components, methods and models designs. The detailed designs of the technological artefacts demonstrate that users are at the centre of system development, and offer both control and transparency over processing of personal data. As a result, this work matches the ambitious goals of the Privacy & Us project.

The commercial transaction working prototypes developed by ESR4 will be further evaluated in lab settings. Each prototype will be evaluated by potential users and the security and privacy related experience gained by the users will be captured. The evaluation results will then be used to identify the transaction design which provides users with high security and privacy related experience.

Furthermore, the technological artefacts App behaviour analyser and privacy risk score component will be validated through experimental and theoretical approaches. The implemented artefact will be examined through experiments in order to test the veracity of theories; and, its applicability will be validated through qualitative and quantitative user studies. In further steps, a potential collaboration has been identified between ERS4 and ESR5. In this respect, a mobile NFC app can be developed using adaptive interfaces that are adjusted according to users' personality to be identified by applying supervised learning. The approach to a system design according to the principles of value-based IT design as proposed by ESR7 will be validated in the iteration two into the Value discovery, Value conceptualization, and Empirical investigation using the iteration one feedback and the first system design. Finally, ESR10 will further investigate and continue to analytically validate the trust establishment model for each participant requirement and to provide a concise argument why the requirements could be fulfilled in the proposed models. Moreover, the data privacy on the level of the application will be studied to define concrete requirements and how would the above model ensure those requirements. Based on the artefacts developed by ESR7 and ESR10, a joint collaboration (paper) describing the abstract trust model in a cars application domain is in progress; additionally, the sealed computation technology is considered in the design of a UBI based on values, which may also include the conceptualization of trust as a required value in the UBI model.

4 References

[1] Sebastian Derikx, Mark de Reuver, and Maarten Kroesen. Can privacy concerns for insurance of connected cars be compensated? Electronic Markets, 26(1):73-81, 2016.

[2] Miremad Soleymanian, Charles Weinberg, and Ting Zhu. The value of usage-based insurance beyond better targeting: Better driving. 2016.

[3] Spiekermann, Sarah. Ethical IT Innovation: A value-based system design approach. CRC Press, 2015.

[4] Dimitris Karapiperis, Birny Birnbaum, Aaron Brandenburg, Sandra Castagna, Allen Greenberg, Robin Harbage, and Anne Obersteadt. Usage-based insurance and vehicle telematics: Insurance market and regulatory implications. Technical Report 1, National Association of Insurance Commisioners (NAIC), 2015. CIPR Study Series.

[5] Siniša Husnjak, Dragan Peraković, Ivan Forenbacher, and Marijan Mumdziev.Telematics system in usage based motor insurance. Procedia Engineering, 100:816-825, 2015.

[6] AS Reddy. The new auto insurance ecosystem: Telematics, mobility and the connected car. Cognizant Reports, 2012.

[7] Friedman B., Peter Kahn, and Alan Borning. Value sensitive design: Theory and methods. University of Washington technical report, 02-12, 2002.

[8] Willcocks, L. and D. Mason. 1987. Computerising Work: People, Systems Design and Workplace Relations. London: Paradigm.

[9] Friedman, B., Kahn, P. H., Jr., and Borning, A. Value Sensitive Design and information systems. In Human computer interaction in management information systems: Foundations, 348-372. M.E. Sharpe, 2006.

5 Glossary of Acronyms / Abbreviations

ASP – Application Software Provider
CP – Cloud Provider
ESR – Early Stage Researcher
GUF – Goethe University Frankfurt
GUI – Graphical User Interface
NFC – Near-field communication
OS – Operating System
PII – Personal Identifiable Information
SVM – Support Vector Machines
TAU – Tel Aviv University
UBI – Usage-Based Insurance
UCL – University College London
UML – Unified Modeling Language
UNI – UNiSCON
USE – USECON Usability Consultants GmbH
VBD – Value-based IT design
VDS – Vasco Group
WP – Work Package