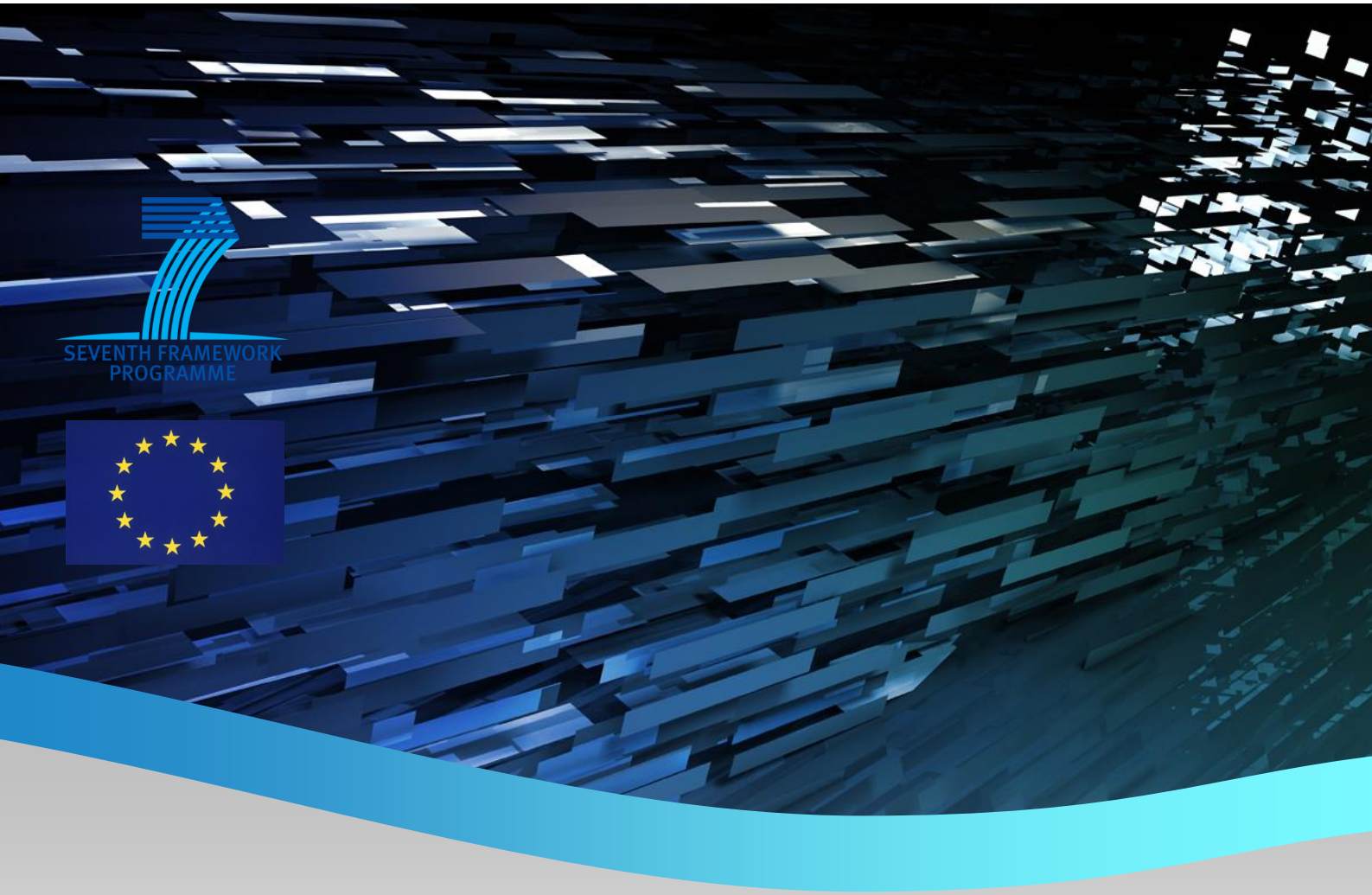

ATTPS | Achieving The Trust Paradigm Shift

Deliverable D2.2 User Experience

Version 1.0

Lydia Kraus - Hanul Sieger - Robert Schmidt - Ina Wechsung - Sebastian Möller - Niklas Kirschnick

30/10/2015

Document Status Report

V.	Date	Document	Editor(s)	Reviewer(s)	Changes
0.1	27/08/2013	Table of Content	Lydia Kraus		
0.2	10/01/2014	Initial Version	Lydia Kraus		
0.3	09/09/2014	Incremental improvement	Lydia Kraus		
0.4	26/11/2014	Incremental improvement	Lydia Kraus		
0.5	17/03/2014	Incremental improvement	Lydia Kraus		
0.6	19/05/2015	First Draft	Lydia Kraus	Roger Berkley	
0.7	15/06/2015	Post Internal Review	Lydia Kraus		Incorporated comments from internal review
0.8	15/08/2015	Post Interim Review	Lydia Kraus		Addressed comments from interim review, restructured document
0.9	15/09/2015	Incremental improvement	Lydia Kraus		Incorporated Interview results and results from the online study
0.9	15/10/2015	Incremental improvement	Lydia Kraus	Roger Berkley	Minor corrections
1.0	30/10/2015	Release	Lydia Kraus		Final

Table of content

List of Figures

List of Tables

Abbreviations

DoW	Description of work
GUI	Graphical User Interface
P&S	Privacy and security
UI	User Interface
UX	User Experience
MPS	Mobile Payment System

1. Introduction

On 24 November 2008, Philips, Microsoft, Nokia and Gemalto took the initiative to establish the Trust in Digital Life (TDL) Partnership. Currently, this TDL partnership is comprised of more than 30 members, observers and associates and is growing steadily.

In 2010, the coordination action ACTOR (ACcelerate Trust in Digital Life Organisation and Relations), started with the aim of improving the organisation, governance, relations of the community, contribute to the research and technological development policy for trustworthy ICT products and services. The main outcomes of ACTOR are the development of the Trust in Digital Life Community: a cross sector and cross boarder ecosystem, the definition of a shared vision, strategy and roadmap action plan reflected in the TDL's Strategic Research and Innovation Agenda (SRA).

The TDL community has developed into an ecosystem with sufficient critical mass that can be used as public platform to discuss and test necessary innovations to speed up the adoption rate of trustworthy ICT and increase user awareness and acceptance.

Achieving The Trust Paradigm Shift (ATTPS) supports the Trust in Digital Life Partnership trust paradigm shift by driving the identified roadmaps of research and deployment projects and monitoring their impact, investigating possible bottlenecks and solutions to overcome them, raising awareness of trustworthy ICT and actively contributing to interoperability and standardisation at European level.

Establishing trust is essential to releasing the full potential of an information-based economy. It is imperative that within the European context, protection of privacy and other basic related human rights of citizens in the future are enhanced and guaranteed and must also apply to the digital world.
Too many technology and service providers perceive investments insecurity and privacy technology to increase of trust as costs which hamper rather than promote business. As a result, many new solutions and services do not include security and privacy features or options. If at all, privacy security is an afterthought, far away from security and privacy by design.

For this reason, the transparent payment for a trust scheme becomes an enabler to move people (consumers, business users), SME's and enterprises towards the mind-set that trust has a value, and would offer the option to 'pay' for trustworthy ICT solutions for a wide range of application domains. Payment can be in money (for most people direct awareness) or by privacy (for most people indirectly aware), as long as it is transparent to the user and there is true choice on how to 'pay' (i.e. what will be done by the gathered data if paid in privacy data) which will also depend on the domain.

One of the objectives of ATTPS is to create awareness at industry, institutes, and governments across member states by means of **identifying consumer** and industry **needs through applying usability lab & living lab methods**.

This objective is addressed in Task 2.1 "User experience: Usability Lab & Living Labs" of Work package 2. Within task 2.1 consumer issues in terms of usability and user experience have been identified within the given subtasks:

- Development of a survey design to test security designs concerning usability, privacy, and trust.
- Presentation of a reference design for trustworthy and usable security for a mobile payment system

The results of the first two subtasks served as an input for the third subtask which is the

- Implementation of a low-cost software solution to aid software architects and programmers to design usable and secure applications.

In the deliverable at hand the results of Task 2.1 are reported:
A survey design to test security designs concerning usability, privacy and trust was developed and iteratively tested in different end-user studies. Thereby, insights into consumers' knowledge/awareness levels, feelings and needs were gained. Moreover, the studies give examples of contexts in which the questionnaires of the survey design could be employed (Section 3 and 4).

Besides applying an iterative testing procedure for the survey design, the conducted studies served to further explore factors which influence related user behavior.

During the last years, a series of studies on mobile payment systems was conducted. The outcome of these studies is summarized in a reference design for trustworthy and usable security for a mobile payment system (Section 5).

The lessons learned during the project and the conclusions are provided in Section 6.

The learnt lessons were used to provide a prototype of a dashboard to help software architects and programmers to include usability and user experience issues into the development cycle (cf. Appendix).

2. Usability, User experience, Security, Privacy and Trust

Before detailing the survey design and the user studies which were conducted within ATTPS and their results, a short overview of usability and user experience in the context of security and privacy (i.e. trustworthy ICT) is given.

Usable security and privacy is focused on investigating system design and user interaction in order to improve the usability of the system and to support security-conform user behavior.

Security and privacy enhancing systems are complex. Besides the complexity of technical implementations, designers of usable security systems face a variety of challenges.

First of all, security and privacy usually require an additional effort which does not relate to the primary goal intended by the user. Therefore, security and privacy are often considered as conflicting with the primary task and being only "secondary goals" (Cranor & Garfinkel, 2005), (Garfinkel & Lipford, 2014); often the design process and implementation of security and privacy solutions occurs after the core functionality of a system was implemented.

The topic of usability, security and privacy has been widely discussed in research during the last decade (cf. e.g. (Garfinkel & Lipford, 2014)). Thereby, the focus has been on making the conflict between usability and security/privacy salient, on improving security and privacy mechanisms regarding usability, and on investigating why users do not sufficiently use security mechanisms and follow security advice.

For instance, Egelmann et al. (2008) investigated why users ignore browser security warnings. Neglecting of password rules such as not writing down passwords, using the same password for several accounts or choosing easy guessable passwords was explored in Adams and Sasse (1999) and Herley (2009). Gross and Rosson (2005) found that many users do not update security software. Circumventing security mechanisms was detailed in many works such as Whitten and Tygar (1999) and De Witt and Kuljis (2006). Wash (2010) explored the mental models of users regarding home computer security to understand why many users are not using security mechanisms at all.

There are usability heuristics e.g. as provided by Nielsen and Molich (1990) which give developers basic hints on how to generally ensure usability (Nielsen & Molich, 1990). Nevertheless, in principal the usability of a system needs to be determined empirically for each developed system and application.

So far, there do not yet exist usability heuristics for usable security and privacy, however, several lessons how to improve usability of security and privacy mechanisms have been learned from the past (Garfinkel & Lipford, 2014):

- *Reduce decisions to be made by the user*
- *Employ safe and secure defaults*
- *Provide users with better information, not more information*
- *Users require clear context to make good decisions*
- *Information presentation is critical*
- *Education works, but has limits*

Another challenge which designers of usable security systems face is that in most cases user interaction is required to ensure security and/or privacy. This results in the problem that the user is a link in the security chain, often a "weak link" leading to decreased security (Garfinkel & Lipford, 2014).

Another problem which Garfinkel and Lipfort (2014) refer to in their overview of the history of usable security is the **"**Barn Door Property**:** Once information is released, it can't be recovered. While many interactive systems make it possible to recover from errors, recovering from security incidents is fundamentally different." (Garfinkel & Lipford, 2014)

While improving the usability of security and privacy enhancing systems is a huge challenge, researchers have pointed out that a user's interaction should be also considered from a holistic point of view including a broader context and different use situations.

"In daily life, people rarely do activities solely for the purpose of security. Instead most IT-security decisions are part of other activities with other purposes. When analyzing these use situations it is impossible to isolate IT-security tasks or decisions." (Bødker, 2012).

Security is therefore dependent on these use situations and not only on a secure device and the implemented security procedures (Bødker, 2012). While (user) experience-based methods[1] have been broadly applied in the human-computer-interaction (HCI) community (Bargas-Avila & Hornbæk, 2011), Dunphy et al. (2014) note that experience design faces a special challenge when it comes to security and privacy applications as within those applications two kind of users need to be taken into account: the target user and the adversary (Dunphy et al., 2014).

Moreover, experiential methods are often based on qualitative studies. For instance in a literature overview on user experience, Bargas-Avila and Hornbæk (2011) find that besides

[1] The term user experience (UX) is widely used and lacks a clear definition. In some works usability and UX are used interchangeably (Bargas-Avila & Hornbæk, 2011), also in the DoW of this project. In this document, UX is referred to as a "holistic view of users' interaction with interactive products" (Bargas-Avila & Hornbæk, 2011).

questionnaires, qualitative methods such as interviews, user observation, video recordings and focus groups are widely deployed methods to investigate user experience. Those qualitative methods, are often more time-consuming in both, conduction and analysis, compared to data collection with questionnaires.

Another challenge which designers of usable security systems face is thus the context dependence of security and privacy actions and the huge amount of time the investigation of this issue might consume.

In the survey design for ATTPS, many of the above mentioned challenges that designers of usable security solutions face were addressed: to better understand the user and therefore the "weak link" in the security chain, questionnaires to measure intrinsic user characteristics were deployed and experiments were conducted to gain insights into the matter. The "secondary task problem" (Garfinkel & Lipford, 2014) was addressed by considering experiential approaches and thereby especially motivational aspects of user behavior. A questionnaire from the literature was used (Sheldon et al., 2001) to investigate motivational aspects in the context of security and privacy actions. This questionnaire is also a valuable tool when it comes to designing technologies that address user experience (Hassenzahl et al., 2010).

3. Survey design

Figure 1 depicts a simplified schematic overview of a system and the points where users are confronted with security. The system is divided in hardware, operating system (OS), middleware and applications. Application, OS and hardware each provide an interface with which the user can interact. As for the hardware, we consider the interface to be limited to the device's cage. The operating system has a user interface which allows the user to interact with the device. The graphical user interface (GUI) related to the operating system varies (e.g. for Smartphones the design of an Android user interface looks different than the design of an iOS interface or for desktop computers a Windows GUI looks different than a Mac desktop). Likewise, applications provide their own interfaces to the user. Data transmission is not considered in Figure 1.

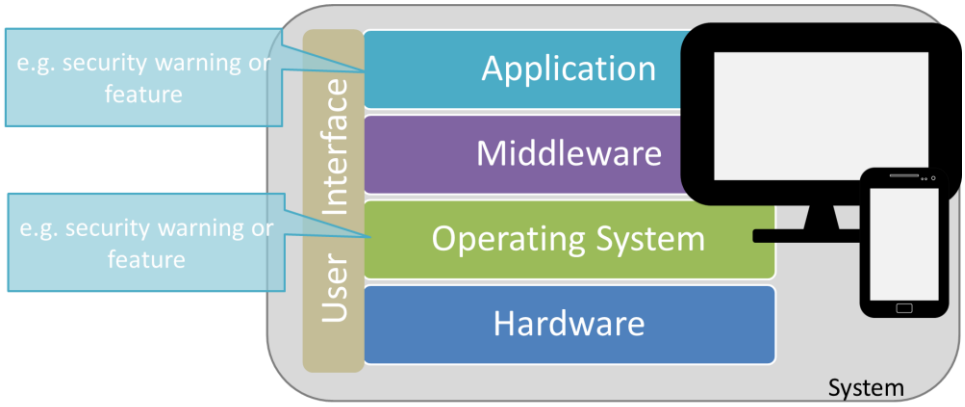

Figure 1 Simplified schematic overview of a technical system and the users' possible perception points of security within the user interface. Security warnings can for instance be initiated by the application itself or on operating system level.

While security is, in the best case, implemented in each part of the system, the user can perceive security (in terms of system characteristics) only if it is part of the user interface (UI) and/or the interaction, respectively. To describe user behaviour Ben-Asher (2011) defines the "triad of security-related behaviour". Thereby, behaviors are divided in three categories: "user's tendency to engage in risky behavior, the use of security features, and the user's response to information from the security system" (Ben-Asher, 2011)). While the first behavior relates to users' intrinsic characteristics, the latter relate to system characteristics.

Regarding information from the security system, for instance, security warnings from operating system (OS) level or the middleware might appear such as permission requests of mobile application (apps). The use of security features, voluntary or forced by the system, includes for instance authentication. Examples of authentication include authentication on the OS level, on the application level or towards remote services.

The generic trust architecture which was developed in ATTPS provides components which address different parts of system security and privacy (cf. Deliverable 3.1). The focus is thereby on the enabling and stimulation of end-to-end trustworthy solutions and their interoperability. The demonstrators which were developed within ATTPS (cf. Deliverable 2.5) showcase examples of systems that include different generic trust architecture components. While some of the demonstrators are back-end applications (e.g. PeFIM), others can be perceived by the user through an interface (Mobile Device Security demonstrator).

Users who are confronted with a system can be asked to judge either the whole system or an application for instance in terms of general ratings, usability, perceived security or privacy, and trust (cf. Figure 2). This approach covers how the system characteristics related to the GUI are perceived by the user.

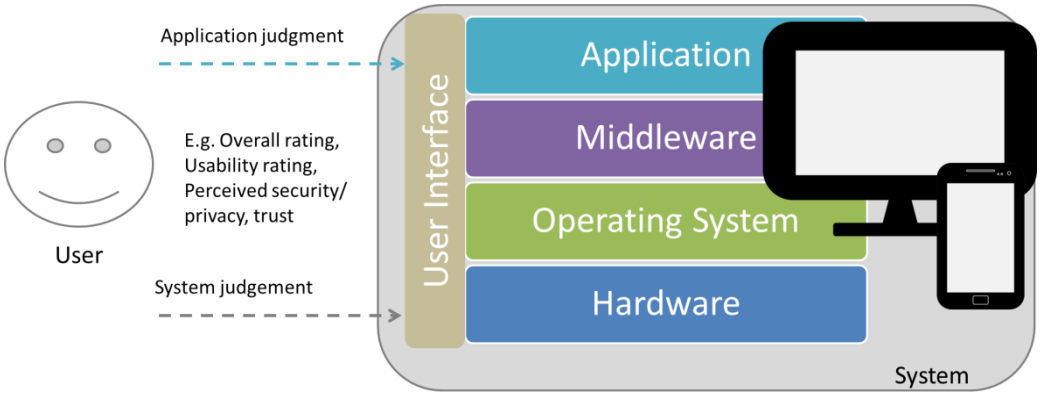

Figure 2 User judgment model

An example for a more holistic view of the user-system interaction is depicted in Figure 3**Error! Reference source not found.**. Thereby, situational factors like motivational aspects, social aspects, threats and their perception by the user and the users' intrinsic characteristics such as personality, privacy concern, knowledge and awareness, and feelings could be considered amongst others.

Within the course of ATTPS, first system characteristics and users' intrinsic characteristics were considered in the survey design. Therefor quantitative studies were conducted to test existing and new questionnaires to measure the issues depicted in Figure 2 and some of the user characteristics. Later on, the survey design was extended to also include a user experience approach. Therefore, qualitative studies were conducted to explore usage situations and experiences. All studies revealed interesting insights into users' behavior,

perception and experiences regarding the usage of security and privacy technologies and actions.

The use cases for the quantitative and qualitative studies focused on mobile security and privacy and digital identity management; thereby, the three core areas of TDL were covered, namely mobile service & platform integrity, trusted stack and data lifecycle management.

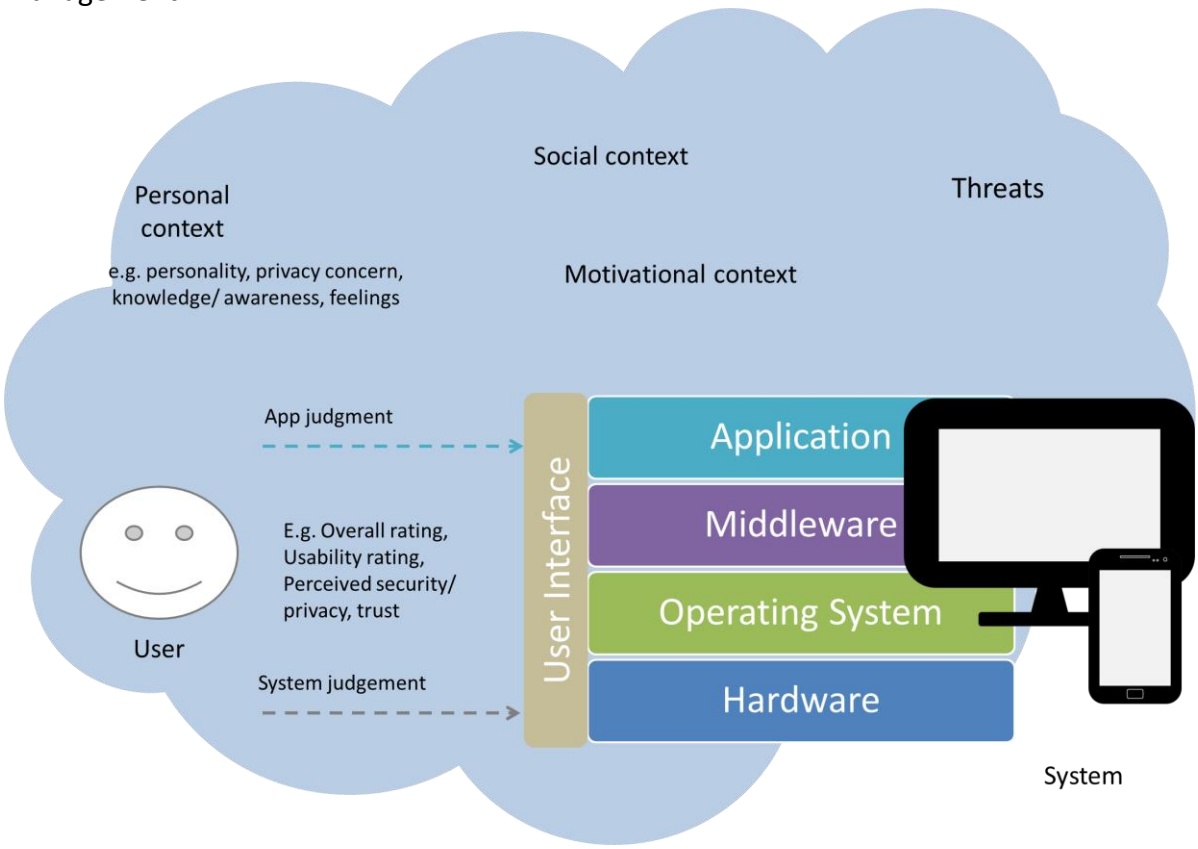

Figure 3 User judgement model in an exemplary usage situation

The hearts of all surveys are questionnaires. Questionnaires measure psychological constructs - the factors which are presumed to have an influence on judgements and behaviors. It is good practice to reuse existing questionnaires which have been proven to measure the underlying constructs with sufficient reliability and validity. If there do not exist questionnaires for factors of interest, new questionnaires need to be developed.

The following questionnaires were deployed during the course of ATTPS and their suitability to examine security designs regarding usability, privacy and trust was determined.

Measuring privacy concern

Privacy concern is a construct which has gained attention in studies of usable security and privacy within the last years.

However, it has been shown in many studies that consumers or users state to be concerned about their (online) privacy but nevertheless, they do not take measures to protect it. This difference between concern and behavior is defined as the privacy paradox: "the mismatch between self-professed privacy attitudes and awareness on the one hand and privacy-undermining behavior on the other hand" (Preibusch, 2013).

For example, in a study conducted by Mylonas et al. (2013) in the context of smartphone security, 95% of the participants stated to be concerned about the "privacy and protection of their personal data", but still the results of the study show that only a small to medium percentage of those participants did something to protect their privacy through smartphone security mechanism (Mylonas et al., 2013)

However, this mismatch should be interpreted with caution. First of all, as also stated in Deliverable 1.2 of this project, users are often missing "the information required to rationally make the necessary trade-offs on a day-to-day basis." (Caballero et al., 2014). Second, scales to determine privacy concern should be selected with care and in the context of the research purpose (Preibusch, 2013). Single questions instruments and instruments with a limited number of questions should be used with caution. One reasons for this is their limited reliability. Another reason is the limited ability to discriminate users based on one question in order to predict behaviour.

Scales with a high number of questions usually offer a better reliability; however one should also pay attention not to overload the study participants.

Preibusch (2013) gives an overview of several scales and their context along with recommendations for choosing the right scale for the right purpose. In the studies conducted within ATTPS, a six item scale, called Global Information Privacy Concern (GIPC) (Malhotra et al., 2004) is used to measure privacy concern. It offers a way to measure general information privacy concern with a relatively low number of items (six).

The GIPC questionnaire was deployed in several experiments and surveys during the course of ATTPS.

Questionnaire (Malhotra et al., 2004)**:**

All things considered, the Internet causes serious privacy problems.[2]								
Strongly disagree	☐	☐	☐	☐	☐	☐	☐	*Strongly agree*

Compared to others, I am more sensitive about the way online companies handle my personal information.								
Strongly disagree	☐	☐	☐	☐	☐	☐	☐	*Strongly agree*

To me, it is very important to keep my privacy intact from online companies.								
Strongly disagree	☐	☐	☐	☐	☐	☐	☐	*Strongly agree*

I believe other people are too much concerned with online privacy issues.								
Strongly disagree	☐	☐	☐	☐	☐	☐	☐	*Strongly agree*

Compared with other subjects on my mind, personal privacy is very important.								
Strongly disagree	☐	☐	☐	☐	☐	☐	☐	*Strongly agree*

I am concerned about threats to my personal privacy today.								
Strongly disagree	☐	☐	☐	☐	☐	☐	☐	*Strongly agree*

[2] This item has been slightly modified compared to the original questionnaire

Measuring privacy and security knowledge

As raising awareness is an important part of ATTPS, users' knowledge about approaches to protect their security and privacy was included into the survey design.

There were several studies conducted in the past to determine the influence of privacy and security knowledge on related user behavior. Park (2011) developed a questionnaire to measure privacy literacy and related online behavior. The questionnaire is divided in three scales:

- Technical familiarity: including concepts such as HTML, ISP, Cache and Phishing; self-reported by respondents on a six point scale ranging from not familiar at all to very familiar.
- Awareness of surveillance practices: measured on true-false scale with items such as "A company can tell you that you have opened an email even if you do not respond".
- Policy understanding: also measured on a true-false scale with items such as "A website is legally allowed to share information about you with affiliates without telling you the names of the affiliate."

In a survey with more than 400 respondents in the US they found that especially technical familiarity is a significant predictor, whereas surveillance awareness and policy understanding only shows small effects (Park, 2011).

Youn (2009) uses four items to measure self-reported privacy knowledge on

- information use,
- information collection
- and age restrictions among young adolescents.

In a survey among more than 100 middle school students, no significant effect of privacy knowledge on privacy protection behavior was found (Youn, 2009).

Former work concentrates on technical familiarity (Park, 2011), awareness of surveillance practices and information use and collection (Park, 2011), (Youn, 2009) and policy understanding (Park, 2011).

However, as ATTPS consists to a large part of industry partners who provide trustworthy ICT solutions, we consider only measuring users' awareness of information use and collection as not sufficient for ATTPS. A user who is aware of the issues handled in the mentioned questionnaires does not necessarily have to be aware on how to apply trustworthy ICT or which mechanisms to use at all. Furthermore, a questionnaire which measures privacy and security (P&S) knowledge could serve as a tool to assess whether

newly developed technologies can be used without obstacles by both knowledgeable and non-knowledgeable users.

Therefor a short questionnaire to determine users' knowledge about everyday security and privacy advices and concepts was developed during the course of ATTPS.

Questionnaire:
The questions of the P&S Knowledge questionnaire are presented in the following, whereas the first answer is always the one who is considered correctly. In a real experimental setting or survey, the order of the first four items answers must be randomized.

	1. How can a user protect herself against data abuse while surfing in a public network?
☐	Avoid entering sensitive data on websites.
☐	Store the network password on the device
☐	Delete the browser history after surfing
☐	Disable location-based services on the device
☐	Don't know

	2. How can a device be protected from viruses?
☐	Always keep software and operating system up-to-date
☐	Don't enter personal data on websites
☐	Avoid using wireless networks
☐	Only visit websites that were recommended by friends
☐	Don't know

	3. How can a smartphone be protected from malicious apps?
☐	Only install apps from trustworthy sources
☐	Check if the downloaded app provides legal info
☐	Try to use apps only occasionally
☐	Check if the app publisher has a website
☐	Don't know

4.	**When using an online-banking app: how can the user protect herself against threats?**
☐	Secure the app with an additional password
☐	Banking apps are always secure and don't need additional security means
☐	Only use the app in urgent cases
☐	Increase the security by modifying the source code of the app
☐	Don't know

5.	**What is the goal of encrypted data transmission?**
☐	The data can't be eavesdropped
☐	The data is protected against viruses
☐	The data can't be lost during transmission
☐	Only the user herself can see the data
☐	Don't know

6.	**What is malware?**
☐	Software which is unwanted and might be harmful
☐	Software which is not working properly
☐	Software which is automatically updating itself
☐	A faulty technical device
☐	Don't know

7.	**What is phishing?**
☐	The interception of personal information via faked routes
☐	The analysis of user's browsing behavior
☐	The sending of unwanted ads
☐	The uninstalling of software that needs too much resources
☐	Don't know

8.	**What is a social engineering technique?**
☐	To spy out somebody's personal environment online with the goal to use this

	information to undertake criminal activities such as identity theft or fraud
☐	To distribute software-testing tasks to several engineers in order to find security leaks
☐	The development of software for social networks
☐	The development of charitable apps which are free of charge
☐	Don't know

9. What is controlled by privacy settings in social networks?	
☐	The personal information that is shared with other people or apps
☐	The personal information that can be seen by the provider of the network
☐	The user data which is forwarded to other social networks
☐	The user data which can be stored by the provider of the network
☐	Don't know

10. What are web analytics?	
☐	Software which analyzes the behavior of website visitors
☐	Software used by search engines to sort results by relevance
☐	Software which automatically interlinks text on websites
☐	Software, which analyzes HTML code for efficiency
☐	Don't know

11. What is written in a privacy policy?	
☐	If and how a company processes personal information
☐	What the user has to do in order to protect her data
☐	How private data is classified in general
☐	That personal information is always processed in anonymized form
☐	Don't know

Measuring perceived privacy, security and trust

The effort to measure the actual security of a system is subject to the evaluation by security experts. The same applies for the privacy-protection which a system offers.

Perceived security and privacy relates to a system's security and ability to protect privacy as perceived by the user. The users' perception is, however, not necessarily in line with the actual security or privacy-protection of the system.

Perceived security and privacy are rarely measured in usable security studies compared to other factors such as usability ratings, decision factors or decisions themselves. But they were discovered as a factor of interest in many e-commerce studies. A scale for measuring perceived security and privacy was for example developed in Chellapa and Pavlou (2002). However, most of those scales are purely focused on e-commerce, and are therefore only of limited interest for ATTPS as in the project perceived security and privacy should be examined in the context of different applications.

Scale:

A scale adopted from the field of perceived quality (Möller, 2005) was used to measure perceived security, privacy and trust. This scale measures a "gut feeling" of security and privacy as perceived by the user and is not limited to any specific field of application.

An example of how this scale is used in the context of perceived security is given in Figure 4.

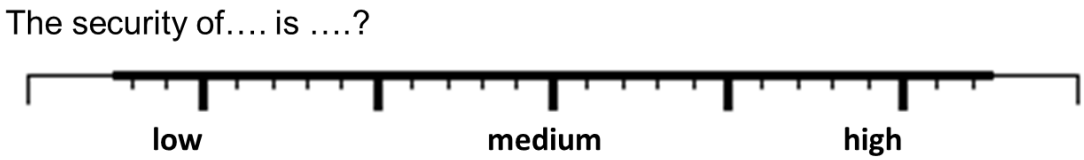

Figure 4 Scale to measure perceived security

The scale was also used to measure the trust a user has in the system.

Measuring usability and user behavior

Usability refers to the “extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use” (ISO 9241-11)

Questionnaires:

Within the course of ATTPS usability was measured with the “System Usability Scale” (SUS) (Brooke, 1996) and the AttrakDiff2 mini questionnaire (Hassenzahl & Monk, 2010). In

Another method to determine the effectiveness or efficiency of a system is to measure user behavior e.g. task completion time, error rate, or success rate. Within ATTPS user behavior was measured in Study 2 with the installation rate of an app (the frequency of installation of an app).

Measuring adoption of mobile protection mechanisms and decision factors

In several of the studies related to mobile security and privacy, a self-developed scale was used to measure mobile protection behavior and factors which play a role in the selection of apps, in general and for messaging apps. The questionnaires used therefor are provided in the following.

Questionnaire 1: Mobile protection behavior

Do you use one or several of the following messaging apps with encrypted data transmission? *(provide examples of current apps of this type)*	
☐	Yes
☐	No
☐	Don't know

Do you use one or several of the following apps to protect you smartphone against threats? *(provide examples of current apps of this type)*	
☐	Yes
☐	No
☐	Don't know

Do you use one or several of the following apps to track your smartphone in case of theft? *(provide examples of current apps of this type)*	
☐	Yes
☐	No
☐	Don't know

Do you use one or several of the following apps to protect your privacy on your smartphone *(provide examples of current apps of this type)*	
☐	Yes
☐	No
☐	Don't know

Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? *(Android users only)*	
☐	Yes
☐	No
☐	Don't know

Did you ever refrain from installing an app due to unusual permissions? *(Android users only)*	
☐	Yes
☐	No
☐	Don't know

Did you ever uninstall an app, after you heard that it is privacy-intrusive?	
☐	Yes
☐	No
☐	Don't know

Questionnaire 2: Decision factors for installing an app (general)

How important are the following factors for your decision to install an app?							
	Not impor-tant at all 1	2	3	4	5	6	Very import ant 7
Description of the app	☐	☐	☐	☐	☐	☐	☐
Visual impression of the app	☐	☐	☐	☐	☐	☐	☐
Reviews provided by other users	☐	☐	☐	☐	☐	☐	☐
Price	☐	☐	☐	☐	☐	☐	☐
Ratings (number of stars)	☐	☐	☐	☐	☐	☐	☐
Number of downloads	☐	☐	☐	☐	☐	☐	☐
Permissions requested by the app	☐	☐	☐	☐	☐	☐	☐
Provided functionality	☐	☐	☐	☐	☐	☐	☐
Publisher (company)	☐	☐	☐	☐	☐	☐	☐

Questionnaire 3: Decision factors for installing a messaging app

How important are the following factors for your decision to install a messaging app?							
	Not impor-tant at all 1	2	3	4	5	6	Very import ant 7
Description of the app	☐	☐	☐	☐	☐	☐	☐
Visual impression of the app	☐	☐	☐	☐	☐	☐	☐
Reviews provided by other users	☐	☐	☐	☐	☐	☐	☐
Price	☐	☐	☐	☐	☐	☐	☐
Ratings (number of stars)	☐	☐	☐	☐	☐	☐	☐
Number of downloads	☐	☐	☐	☐	☐	☐	☐
Permissions requested by the app	☐	☐	☐	☐	☐	☐	☐
Provided functionality	☐	☐	☐	☐	☐	☐	☐
Publisher (company)	☐	☐	☐	☐	☐	☐	☐
Distribution within my circles	☐	☐	☐	☐	☐	☐	☐
Message encryption	☐	☐	☐	☐	☐	☐	☐
Ease of use	☐	☐	☐	☐	☐	☐	☐

Measuring factors for intrinsic motivation: psychological need fulfillment

Experiential approaches help to gain a "rich understanding of people's practices and lives" (Dunphy et al., 2014). However, while experiential approaches such as interviews and focus groups are insightful on the one hand, they are time-consuming on the other hand. Quantitative alternatives to investigate aspects of user experience are the AttrakDiff2 questionnaire (Hassenzahl & Monk, 2010) and the theory of psychological needs in the context of interactive products (Hassenzahl, 2010).

Psychological needs and user experience

According to Hassenzahl et al. the main motivation to use interactive technologies is to achieve a certain experience induced by the fulfilment of a psychological need (Hassenzahl et al., 2010): psychological needs can thus be used to identify classes of experiences.
A user would for instance make a phone call to experience the feeling of being close to others (thus, the motivation would be the fulfilment of the need *Relatedness*), rather than making a phone call for the call's sake (Hassenzahl, 2010). Or, a user could activate the privacy setting in their messaging app so that senders of messages cannot see when a message was read. This would avoid that the sender puts pressure on the user to immediately reply to the message. This way, the privacy setting would be used to fulfill the need of *Autonomy* (defined as "feeling like you are the cause of your own actions rather than feeling that external forces or pressures are the cause of your actions" (Sheldon et al., 2001)).

By classifying experiences according to the psychological needs that motivate them, the complexity of the design space for user experience can be reduced.

The number of needs discussed in the literature varies between 3 and 16 needs ((Ryan & Deci, 2000), (Sheldon et al., 2001), (Reiss, 2004)). However, the mentioned needs overlap to a large part (Fronemann & Peissner, 2014). Psychological need fulfillment has shown to influence users' ratings of a products' hedonic quality depending on the attribution, i.e. the degree to which users deem the product responsible for the experience (Hassenzahl et al., 2010). Hedonic quality is one of the constructs which is measured in the AttrakDiff questionnaire (cf. Section "Measuring usability and user behavior").

To further explore usage situations and get insights into consumers' motivation to perform security and privacy actions, we applied the need questionnaire provided in (Sheldon et

al.,2001) plus several items for measuring the need of "Keeping the meaningful" from the UNEEQ questionnaire[3].

Table 1 provides and overview of the different needs. Definitions are taken from (Sheldon et al., 2001). Definitions for "Keeping the meaningful" are taken from (Fronemann & Peissner, 2014) and (Reiss, 2004).

Autonomy	Feeling like you are the cause of your own actions rather than feeling that external forces or pressures are the cause of your actions.
Competence	Feeling that you are very capable and effective in your actions rather than feeling incompetent or ineffective.
Relatedness	Feeling that you have regular intimate contact with people who care about you rather than feeling lonely and uncared for.
Self-actualization	Feeling that you are developing your best potentials and making life meaningful rather than feeling stagnant and that life does not have much meaning.
Security	Feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances.
Money/ Luxury	Feeling that you have plenty of money to buy most of what you want rather than feeling like a poor person who has no nice possessions.
Physical/ Bodily	Feeling that your body is healthy and well-taken care of rather than feeling out of shape or unhealthy.
Self-esteem	Feeling that you are a worthy person who is as good as anyone else rather than feeling like a "loser".
Stimulation	Feeling that you get plenty of enjoyment and pleasure rather than feeling bored and understimulated by life.
Keeping the meaningful	Collecting meaningful things / saving

Table 1 Overview of basic psychological needs. Definitions taken from (Sheldon etal., 2001), (Fronemann & Peissner, 2014) and (Reiss, 2004).

Within ATTPS the need questionnaire was deployed in the context of security and privacy. The questionnaire is provided in the following.

3 http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf

ATTPS | Achieving The Trust Paradigm Shift

Need Questionnaire (Sheldon et al., 2001)**:**

During this event I felt. . .

Autonomy

… that my choices were based on my true interests and values. (AUT 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… free to do things my own way. (AUT 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that my choices expressed my "true self." (AUT 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Competence

… that I was successfully completing difficult tasks and projects. (COMP 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that I was taking on and mastering hard challenges. (COMP 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… very capable in what I did. (COMP 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Relatedness

… a sense of contact with people who care for me, and whom I care for. (REL 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… close and connected with other people who are important to me. (REL 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… a strong sense of intimacy with the people I spent time with. (REL 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

ATTPS | Achieving The Trust Paradigm Shift

Self-actualization/ meaning

… that I was "becoming who I really am." (SA 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… a sense of deeper purpose in life. (SA 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… a deeper understanding of myself and my place in the universe. (SA 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Security/Control

… that my life was structured and predictable. (SEC 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… glad that I have a comfortable set of routines and habits. (SEC 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… safe from threats and uncertainties. (SEC 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Money/ Luxury

… able to buy most of the things I want. (LUX 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that I had nice things and possessions. (LUX 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that I got plenty of money. (LUX 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Influence/ Popularity

… that I was a person whose advice others seek out and follow. (POP 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that I strongly influenced others' beliefs and behavior. (POP 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that I had strong impact on what other people did. (POP 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Pleasure/ Stimulation

… that I was experiencing new sensations and activities. (STIM 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… intense physical pleasure and enjoyment. (STIM 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… that I had found new sources and types of stimulation for myself. (STIM 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

Keeping the meaningful[4]

… I was collecting meaningful things (MEAN 1)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… I was keeping meaningful things (MEAN 2)						
Not at all	☐	☐	☐	☐	☐	*Very much*

… I was keeping record of important things (MEAN 3)						
Not at all	☐	☐	☐	☐	☐	*Very much*

[4] Items for "keeping the meaningful" were taken from the UNEEQ questionnaire: http://www.hci.iao.fraunhofer.de/content/dam/hci/de/documents/UXellence_UserNeedsQuestionnaire_EN.pdf

Conducted user studies

Several studies were conducted during the course of ATTPS. The results of the studies were presented at various opportunities to academic and industry-related audience. Table 2 gives an overview of the conducted studies and the questionnaires which were employed in each study.

Measured construct	Study 1	Study 2	Study 3	Study 4	Study 5	Study 6	Mobile Paym.
Usability measures							
System Usability Scale (SUS)	-	-	-	-	-	-	yes
Pragmatic and Hedonic Quality (AttrakDiff)	-	-	-	-	-	-	yes
Usability measures w.r.t. user behavior	-	yes	-	-	-	-	-
Adoption							
Mobile protection behavior	yes	yes	-	-	-	yes	-
Decision factors for installing an app	yes	yes	-	-	-	-	-
Decision factors for installing a messaging app	-	-	-	-	-	yes	-
Perception							
Security	-	-	-	-	-	-	yes
Privacy	-	yes	-	-	-	-	-
Trust	-	yes	-	-	-	-	-
Intrinsic Factors							
Privacy Concern (GIPC)	yes	yes	-	-	-	-	-
Privacy and Security Knowledge (P&S Knowledge)	yes	-	-	-	-	-	-
Personality traits (BIG Five)	-	-	-	-	-	-	yes
Domain-Specific Risk-Taking (DOSPERT-G)	-	-	-	-	-	-	yes
Technical affinity - electronic devices (TA – EG)	-	-	-	-	-	-	yes
Need fulfillment							
Psychological need fulfillment	-	-	-	-	-	yes	-

Table 2 Overview of conducted studies and deployed questionnaires

Each quantitative study (study 1, 2, 6 and the studies conducted for the mobile payment reference design) represents a test of the questionnaires in different contexts. Moreover, the studies give examples of how the interplay between different variables in the context

of usability, privacy and trust could look like. The qualitative studies (study 3, 4 and 5) further explore the framework for usability, privacy and trust in order to find variables and questionnaires of interest which have not been considered so far (such as motivation). While the experiments that led to the mobile payment reference design were rather focused on usability and user characteristics, we decided to concentrate in the survey design on privacy and security knowledge and privacy concern. The reason for this is that awareness (which is closely related to knowledge) plays a major role within ATTPS. Moreover, privacy concern has gained much attention during the last years. A search on google scholar shows 10.600 results when the term “privacy concern” is entered (as of the beginning of October 2015, cf. Appendix). This is more than twice as much as the results until 2011 (5.230 results).

Study 1: Development of a Privacy and Security Knowledge Questionnaire

ATTPS consists to a large part of industry partners who provide security solutions. Therefore, we consider it crucial to measure users' knowledge about how they could protect themselves from threats. We envision the privacy and security (P&S) knowledge questionnaire as an instrument to segment groups of users. It should serve as a tool for developers of security and privacy-enhancing technologies to assess whether newly developed technologies can be used without obstacles by both knowledgeable and non-knowledgeable users.

Study 1: Design of the questionnaire and the survey to test it

The development of the questionnaire was started by collecting items (questions) for the questionnaire. Therefore we accessed several webpages and sources with security recommendations for users during 2013 and 2014 (Data Privacy Day, 2014; Hogben & Dekker, 2010; 4 safety tips for using Wi-Fi, 2014; How to Make Smart Wireless Choices and Avoid Problems, 2014).

We collected 27 recommendations from which we derived a list of items. In addition, four experts met in a brainstorming session to determine P&S concepts to be used in the questionnaire. After the expert session **24 multiple choice items** were left. Each item consists of one question and four suggested solutions of which three are wrong and one is correct plus an additionally "don't know" option as an answer.

An online study with 154 participants was then conducted to test the questionnaire. Thereby the item difficulty (i.e. the percentage of participants that were able to correctly answer the question) and the reliability of the questionnaire were examined. A detailed description of the results is provided in Kraus et al. (2014 a). These values provided the basis to select the best items.

The finally selected **11 items** of the P&S knowledge questionnaire and the respective answers can be found in Section 3.

Besides the questions on P&S Knowledge we asked the participants questions on demographics, internet usage, smartphone usage, privacy concern, and mobile protection behavior. The Global Information Privacy Concern (GIPC) questionnaire which is provided in Malhotra et al. (2004) was used to measure privacy concern. The answer scale was a 7-point scale from 1 = *strongly disagree* to 7 = *strongly agree*. Mobile protection behavior was measured with a set of self-developed questions. The purpose of measuring other variables than only knowledge was twofold. First, demographic questions and questions about technology usage describe the characteristics of the sample and provide data on how P&S knowledge is related to demographics and technology usage. Second, the questions about privacy concern and mobile protection behavior served to examine

relations between knowledge and concern and between knowledge, concern and behavior (note that a limitation hereby is that reported behavior can differ from the actual behavior).

The questions about mobile protection behavior were the following:

- Do you use one or several of the following messaging apps with encrypted data transmission? (Secure messenger apps)
- Do you use one or several of the following apps to protect you smartphone against threats? (Anti-virus apps)
- Do you use one or several of the following apps to track your smartphone in case of theft? (Anti-theft apps)
- Do you use one or several of the following apps to protect your privacy on your smartphone? (Privacy protection apps)
- Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? (Refrain – high number of permissions)
- Did you ever refrain from installing an app due to unusual permissions? (Refrain – unusual permissions)
- Did you ever uninstall an app, after you heard that it is privacy-intrusive? (Uninstall – privacy intrusiveness)

Study 1: Participants

The survey was completed by 154 participants between 18 and 59 years old (M = 29.61, SD = 9.19). They were recruited on an online portal for voluntary study participants hosted by TU Berlin. 67 participants (43.2%) were male and 86 (55.5%) were female, 2 (1.3%) did not report their gender. (cf. Figure 5)

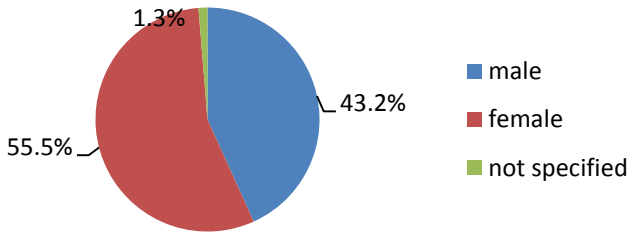

Figure 5 Gender distribution

Participants with less than a secondary school degree (15.4%), secondary school degree (43.2%), and university degree (41.3%) were represented; there was a bias towards higher educational levels.

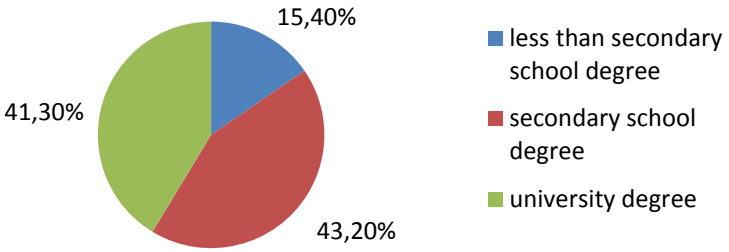

Figure 6 Educational groups

Various occupational groups were represented with a bias towards students (54.2%). 35 participants (22.7%) had professional IT expertise, whereas 119 participants (77.3%) did not have professional IT expertise. Current and past work in a profession related to IT, computer science, communications engineering, and similar professions were considered IT expertise. Also students of these areas were considered as having professional IT expertise. The majority (N=137, 89%) of participants were smartphone users (Android (N=88, 56.8%), iOS (N=41, 26.5%), "Other" (N=8, 5.8%), cf. Figure 7).

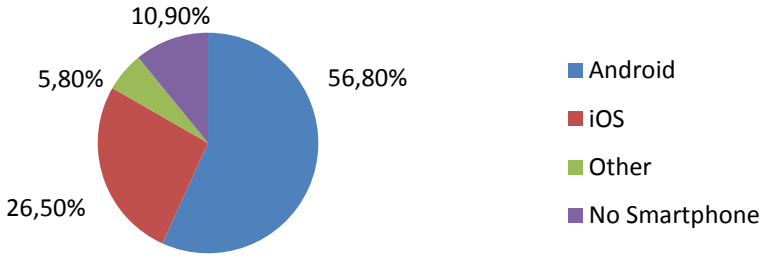

Figure 7 Distribution of smartphone OS' among study participants

Study 1: Results

In the following we summarize the results of the survey. A detailed overview of the results and of the statistical tests is given (Kraus et al, 2014 b).

24 items of the P&S Knowledge Questionnaire were tested and based on the item difficulty 11 items were selected to remain in the questionnaire. The questionnaire has an acceptable KR-20 reliability of 0.67.

A P&S Knowledge score was calculated for each participant as the sum of correctly answered questions. Afterwards, based on the quartiles of the descriptive statistic, the participants were divided in groups of low, medium and high knowledge. An overview of the descriptive statistics is given in Table 3.

Table 3 Descriptive statistics for P&S knowledge and privacy concern (PC) score

	Min	1st Quartile	Mean	Median	3rd Quartile	Max
P&S (*N* = 154)	1	6	7.71	8	9	11
PC (*N* = 154)	1	4	4.75	4.83	5.54	7

χ^2-tests and corresponding Phi-coefficients were used to determine if there are associations between the demographics and the P&S knowledge level. **Significant relations between gender, educational level and IT expertise were found.** Male participants were less likely to have low P&S knowledge, whereas female participants were less likely to have high P&S knowledge compared to the complete sample. Participants who had less than a secondary high school degree were more likely to have low P&S knowledge and less likely to have high P&S knowledge compared to the complete sample. Participants without IT expertise were more likely to have low and medium P&S knowledge, whereas participants with IT expertise were less like to have low or medium P&S knowledge compared to the complete sample. **There was no correlation between P&S knowledge and age.**

Also, the study shows that there are differences in the behavior between the groups of low, medium and high P&S knowledge (cf. Table 4). For 4 of 5 protection questions, participants with high P&S knowledge were more likely to report this behavior compared to the complete sample. The results suggest that a **lack of knowledge is currently an obstacle** when it comes to adopting mobile security mechanisms.

Table 4 Differences in behavior between different groups of P&S knowledge[5]

Behavior	P&S Knowledge
1. Do you use one or several of the following messaging apps with encrypted data transmission? (Yes[6] = 19%)	**high ↑; low ↓** $\chi^2(2, N=137) = 10.37$; $p=0.005$
2. Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? (Yes[1]: 62.8%)	**high ↑** $\chi^2(2, N=135) = 7.23$; $p=0.027$
3. Did you ever refrain from installing an app due to unusual permissions? (Yes[1]: 75.9%)	-
4. Did you ever uninstall an app, after you heard that it is privacy-intrusive? (Yes[1]: 45.3%)	**high ↑; medium ↓** $\chi^2(2, N=135) = 7.83$; $p=0.021$

[5] For cases 1-4 only smartphone users were considered. "low", "medium" and "high" indicate the P&S knowledge or privacy concern group. Groups and behaviors without significant differences are not reported. The arrows indicate whether a group was either more likely to report a specific behavior (↑) or less likely (↓) compared to the complete sample (post-hoc tests with Bonferroni-correction).
6 Refers to all smartphone users in the sample.

5. Do you use the private browsing function of your browser? (Yes[7]: 33.6%)	**high ↑** $\chi^2(2, N=154) = 10.56$; $p=0.005$

Ideally, trustworthy ICT solutions should be designed in such a way that there is no difference in the adoption between users of high, medium and low P&S knowledge. To ensure that this difference is eliminated, developers should already during the design of trustworthy ICT solutions pay attention, that the functionality and the benefit of the solution are easily understandable for potential users.

The developed questionnaire can be used to measure the P&S knowledge of users in user studies related to the design of trustworthy ICT and to examine whether there is a difference in the behavior (e.g. willingness to adopt or willingness to pay for a solution) between users of different knowledge levels.

The study in section 4.1.1 shows that there are differences between users of low, medium and high P&S knowledge level regarding the adoption of security mechanisms. To avoid this in the future, the questionnaire can serve as a starting tool to assess whether a developed technology is subject to differences in adoption depending on the knowledge level.

7 Refers to the complete sample

Study 1: The influence of privacy concern

It was mentioned before that privacy concern is a construct which has gained attention in studies of the usable privacy and economics of privacy community within the last years. Even though privacy concern shows to be a limited predictor of behavior in many cases, we assume that, when measured with care, i.e. by not relying on single question instruments and providing graded answer options instead of yes/no answer options, it might serve as a predictor.

Moreover, the relation between privacy concern and P&S knowledge has been little investigated so far. Does it make sense to measure both in order to predict user behavior? Or is one of them enough as they are highly correlated?

As both, privacy concern and P&S knowledge, were measured in the online study described in the subsection on study 1 before, the data of the study can also be analyzed according to this question. Besides differences in the behavior between participants with low, medium and high **P&S knowledge**, the study shows that there are also differences in the behavior between the groups of low, medium and high **privacy concern** (cf. Table 5).

A detailed analysis of the study results is provided in Kraus et al. (2014 b).

Table 5 Differences in behavior between different groups of privacy concern

Behavior	Privacy Concern
1. Do you use one or several of the following messaging apps with encrypted data transmission? (Yes[1] = 19%)	**low ↓** $\chi^2(2, N=137) = 6.62$; $p=0.041$
2. Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? (Yes[1]: 62.8%)	**low ↓** $\chi^2(2, N=135) = 6.04$; $p=0.041$
3. Did you ever refrain from installing an app due to unusual permissions? (Yes[1]: 75.9%)	**low ↓** $\chi^2(2, N=135) = 13.94$; $p=0.001$
4. Did you ever uninstall an app, after you heard that it is privacy-intrusive? (Yes[1]: 45.3%)	**high ↑; low ↓** $\chi^2(2, N=135) = 12.04$; $p=0.002$
5. Do you use the private browsing function of your browser? (Yes[2]: 33.6%)	-

An overview of the reliability measures of the GIPC scale (determined in the quantitative studies) is given in Kraus et al. (2014 b). Values for Cronbach's alpha range between 0.75 (original study) and 0.89 (AppChoice study), indicating that the questionnaire measures global privacy concern with good reliability.

Study	Sample Size (N)	Mean (Privacy Concern)	Standard Deviation (Privacy Concern)	Reliability
Malhotra et al. (2004)	449	M = 5.01	SD = 1.29	Composite reliability (CR) = 0.75
Study 1	154	M = 4.75	SD = 1.14	Cronbach's alpha = 0.80
Study 2	48	M = 4.19	SD = 1.05	Cronbach's alpha = 0.89

Table 6 Reliability measures for GIPC

Study1: Conclusion

The analysis shows that P&S knowledge and privacy concern are not correlated, but both are influential for mobile protection behavior (cf. Table 4 and Table 5). Whereas high P&S knowledge serves rather as a predictor for the adoption of mobile security mechanisms, low privacy concern serves as a predictor for refraining from the usage of those mechanisms. Thus, participants with high privacy concern were **not** more likely to have adopted security mechanisms, but those with high P&S knowledge were.

This is an interesting observation as it suggests that influencing users' privacy concern might not help as much to support adoption of trustworthy ICT as influencing their knowledge. Moreover, in contrast to privacy concern, P&S knowledge can be easily influenced by educating users and giving them concrete advice on how to protect their devices.

Still, it makes sense to measure both constructs in order to get a more fine-grained segmentation of user groups and their trustworthy ICT-related behavior. However, when it comes to manipulating one of the two variables, it makes more sense to influence knowledge than concern. This is in line with the goal of ATTPS and TDL, namely to increase awareness. The awareness raising should thereby concentrate on the education of stakeholders regarding available trustworthy ICT solutions and their proper deployment rather than on potential threats to security and privacy.

Study 2: Testing the influence of alternative user interfaces for Android app permissions on the perceived privacy of and trust in applications

The following study demonstrates the possible relations among some of the influencing factors in the survey design (perceived privacy, trust, user interface) and the user behavior (adoption or in this case decision to install a mobile app) with an example from smartphone security.

Detailed results of the user study are reported in Kraus et al. (2014 c).

Study 2: Design of the study

Android is open for third-party app providers and provides a permission-based security system to control the access of third party apps to privacy- and security critical resources. Former studies show that most users have difficulties to understand the permission dialogue and that many of the users do not pay attention to the dialogue at all (Felt et al., 2012 b). Also the permissions are shown to the users after the decision to download an app has already been made and the "install" button has been pressed. Thus, it is difficult for the users to include the permissions into the decision making process without additional effort. Even though Google has modified the presentation of the permissions to be arranged clearer in 2014[8], in the current user interface the permissions are still shown to the user after the decision to download an app has been made.

We address this problem by suggesting two alternative user interfaces which allow the users to make informed decisions regarding the risk that is associated with the permissions. By providing statistics on the number of permissions used by an app in comparison to apps with similar functionality, a context for the decision is provided. Moreover, the information can be included in the decision-making process as it is given before the decision to install an app is made.

Figure 8 shows one of the two user interfaces (UIs). During the study the participants got presented with two apps of similar functionality of which one had a high number of permissions and the other a low number of permissions. The participants were supposed to look at both apps and then to decide which app they would install on their device. There were three experimental conditions: Condition 1, the "Standard UI", presented the participants with the apps as in the Google Play Store to the time when the experiment was conducted (autumn 2013). Condition 2, the "Text UI", presented the apps with a user interface were statistical information was given in form of a text additional to the information provided in the "Standard UI". Condition 3, the "Graphic UI", presented the

8 http://www.citeworld.com/article/2450481/mobile-byod/simplified-android-apps-permissions-will-reduce-user-control.html

participants with the same information as in the standard UI plus additional statistical information in form of a small text and a graphic. All participants were presented all user interfaces in different order (counterbalanced).

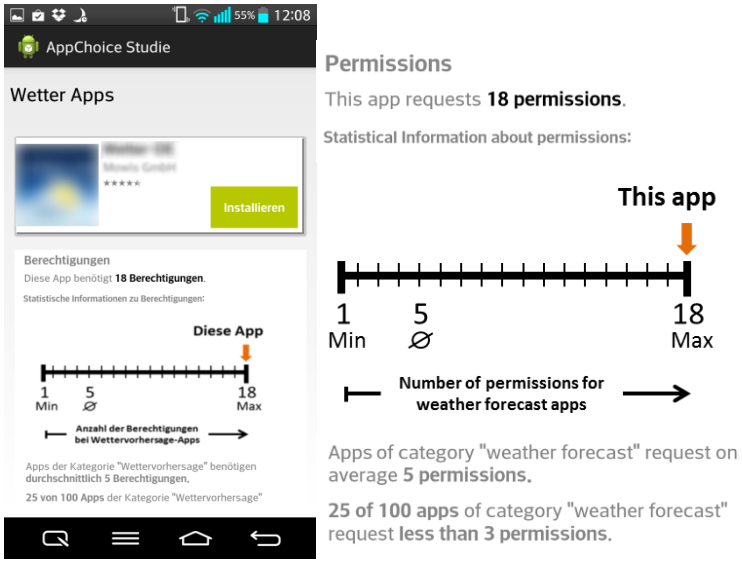

Figure 8 One of the interfaces which provides the statistical information in form of text and graphics

Within the user study the following variables were measured:

- **Demographics:** age, gender, IT-expertise, education, etc.
- **Installation rate:** The percentage of high and low permission apps installed, measured for each UI (i.e. the usability factor in this case)
- **Decision factors:** After each decision the participants rated on a 7-point scale how important each decision factor was for this decision. The decision factors included: the description of the app, the visual impression of the app, the reviews provided by other users, the ratings (number of stars), the number of downloads, the permissions requested by the app, the provided functionality (according to description), the publisher (company)
- **Perceived privacy:** Participants had to rate for both apps (the low and the high permission app) how much they think that the app would protect their privacy
- **General Trust:** Participants had to rate for both apps (the low and the high permission app) how much their trust the app is
- **Privacy concern:** Privacy Concern was measured with the Global Information Privacy Concern scale as provided in Malhotra et al. (2004)

Study 2: Participants

48 Android users participated in the study (24 female). The participants were between 18 and 60 years old with an average of 31.68 years. The Participants has different kinds of school degrees: 33.3% had less than a secondary school degree; 39.65% had a secondary school degree, and 27.1% had a university degree (cf. Figure 9).

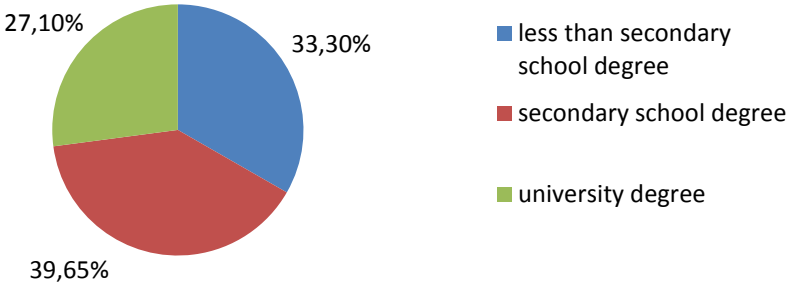

Figure 9 Educational groups in the AppChoice study

There were all kind of occupational groups participating: employees (29.2%), self-employed (8.3%), students (31.3%), apprentices (6.2%), pupils (8.3%), pensioners (4.2%), housewives/-husbands (2.1%), unemployed (6.2%) and others (4.2%) (cf. Figure 10).

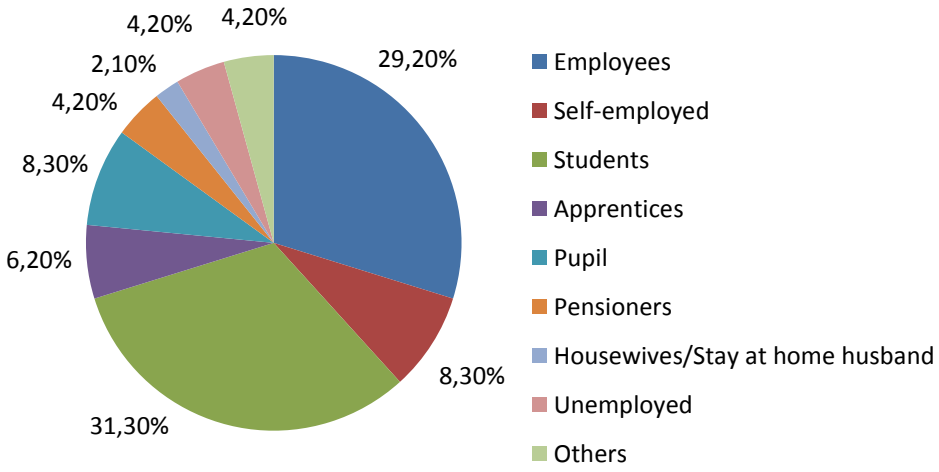

Figure 10 Occupational groups in the AppChoice study

The participants used different kind of devices such as HTC wildfire, HTC desire X, Sony Erricsson XPERIA Arc S, Sony Xperia miro, Sony Xperia Play, Sony Xperia S, Samsung Galaxy Ace, Samsung Galaxy Ace 2, Samsung Galaxy S1 – S4, Samsung Galaxy S3 mini, Samsung Galaxy Nexus, Samsung Galaxy S Plus, Samsung Galaxy S Duos and LG-E610.

Study 2: Results

The experiment showed that for the "Graphic UI" significant fewer participants installed the app with the high number of permissions compared to the "Standard UI" (cf. Figure 11). Also the decision factor "permissions requested by the app" was significant more important for the decisions made when the "Text UI" and the "Graphic UI" were presented compared to the "Standard UI" (cf. Figure 12). Whereas in the "Standard UI" the perceived privacy and trust did not differ significantly between the high- and the low-permission app, in the "Text UI" and in the "Standard UI" the low-permission app had a significantly higher perceived privacy and trust as the high-permission app (cf. Figure 13 and Figure 14).

Detailed results are reported in Kraus et al. (2014c).

Table 7 Numeric Values for Installation rate and importance of permissions

	Standard UI	Text UI	Graphic UI
Installation rate (high perm. app)	43,45%	33.33%	20.83%
Importance of permissions	3.41	5.11	5.41

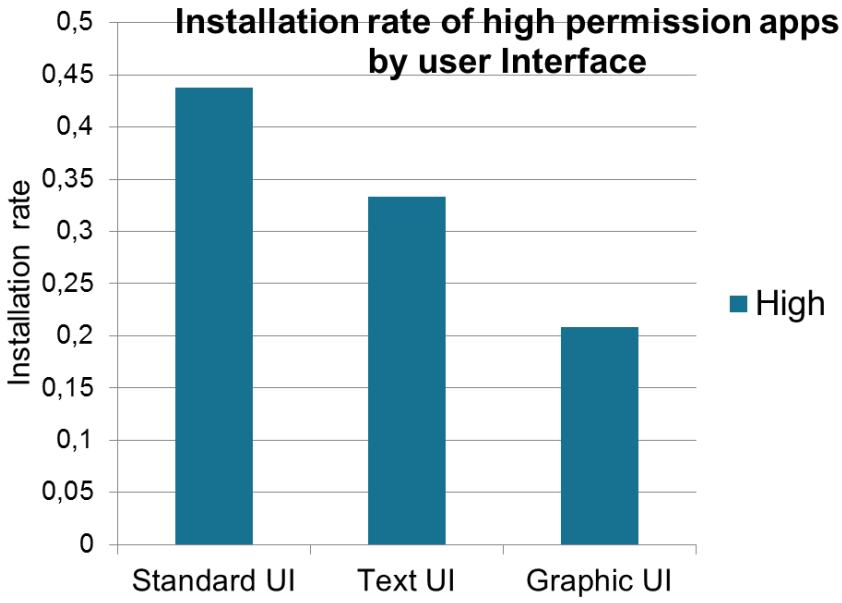

Figure 11 Comparison of installation rates

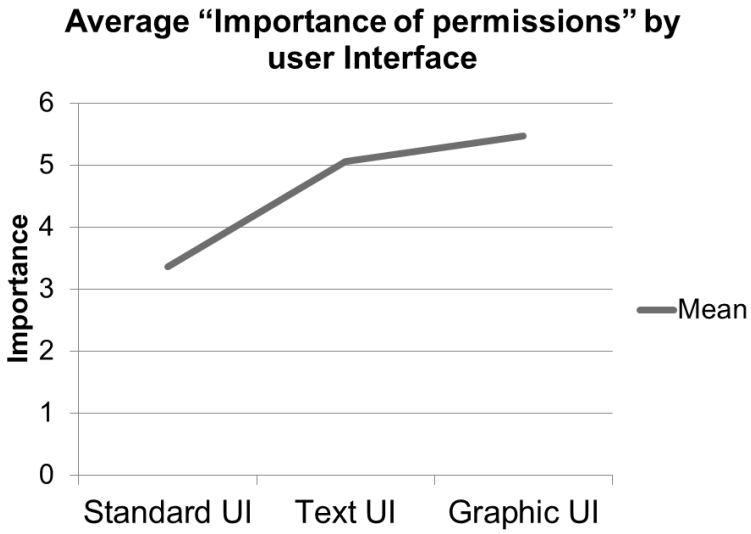

Figure 12 Comparison of permissions as a decision factor

Table 8 Mean values for perceived privacy in the low and the high-permission app

	Standard UI	Text UI	Graphic UI
Perceived privacy (low perm. app)	14.92	17.67	17.74
Perceived privacy (high perm. app)	13.5	8.43	10.87

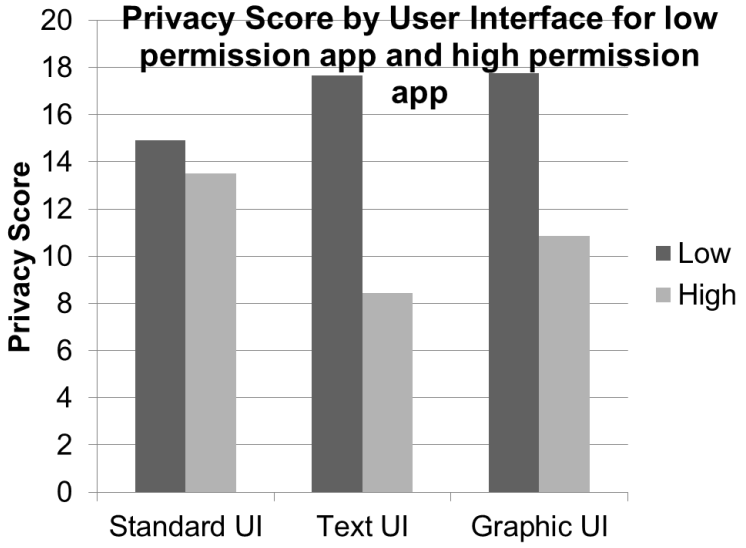

Figure 13 Comparison of perceived privacy

Table 9 Mean values trust in the low and the high-permission app

	Standard UI	Text UI	Graphic UI
Trust (low perm. app)	14.71	17.30	17.59
Trust (high perm. App)	14.12	10.24	11.02

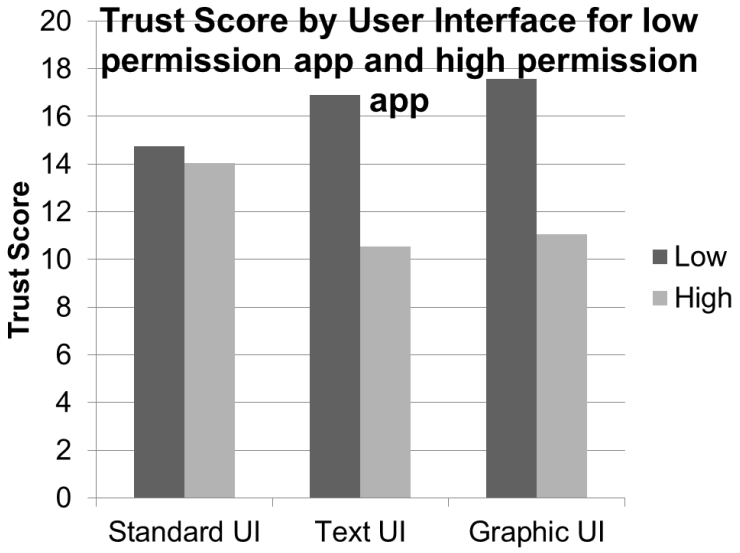

Figure 14 Comparison of perceived trust

Study 2: Conclusion

This example shows that, depending on how information is presented to the user, user behavior is influenced and privacy-intrusiveness and trust are perceived differently. The fact that the users were given a context for the decision suggests that privacy and security, when visible and comparable to competing offers, can influence the decision making.

This was also demonstrated in (Jentzsch et al., 2012) and (Egelman et al., 2013). However, in our case we did not have conditions in which the price of the apps differed. The observed effect might change as soon as the privacy-intrusive offer is cheaper than the non-intrusive offer (Jentzsch et al., 2012).

So far, several quantitative studies were presented in which the questionnaires for measuring P&S knowledge, privacy concern and perceived privacy and trust were deployed. Usability factors were either measured in terms of adoption or installation behavior.
The following qualitative studies further explore influencing factors of user behavior in the context of usability, security, privacy and trust. Moreover, their goal is to gain further understanding of users' perceptions, views and behavior in this context.

Study 3: Digital identity management concept test

The first qualitative study conducted within task 2.1 was a concept test for a digital identity management platform named "Egofy" which is provided by the consortium partner Cryptas. Egofy is an instationation of the Pe-FIM model, described in Deliverable 3.1.

The Egofy platform consists of several components which are also depicted in Figure 15:

- Identity Provider (IdP)
- Identity Federator (IdF)
- Attribute Provider (AP)
- Service Provider (SP)
- Service Broker (SB)
- Federation Operator (FO)

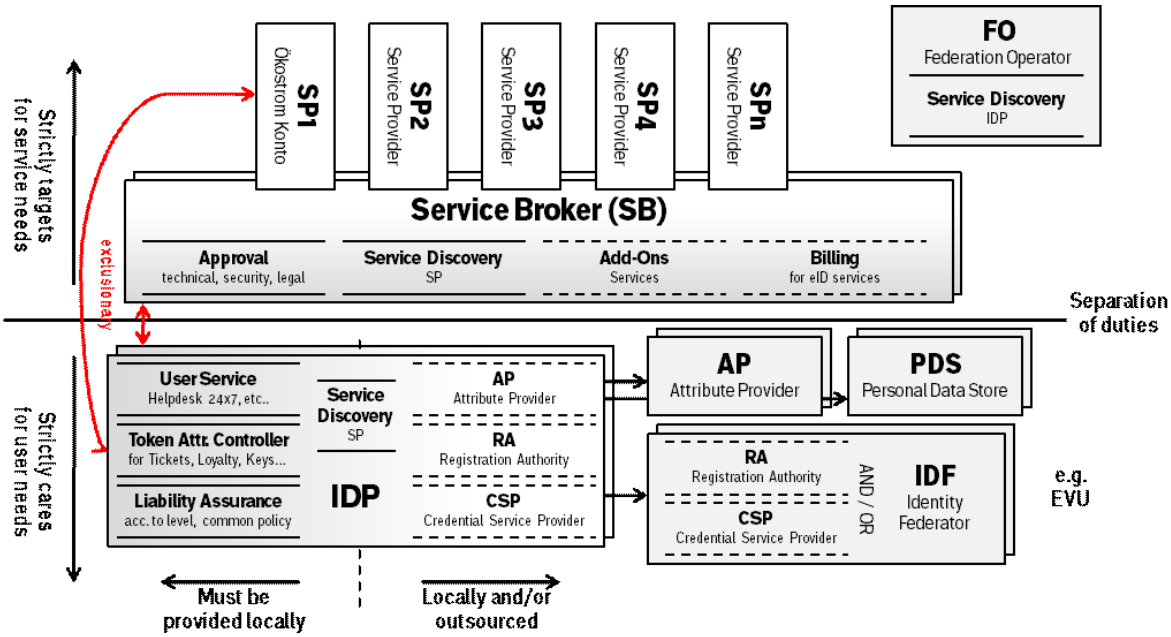

Figure 15 Egofy Architecture (by courtesy of Cryptas)

A detailed overview of the system architecture and conceptual idea is provided in ATTPS-Deliverable 3.1.

Study 3: Design of the study

The objective of the concept study was twofold. The first goal was to gather users' impressions of the conceptual framework of the digital identity management platform "Egofy". Thereby, study participants had to answer questions regarding the judgment of the idea (e.g. What is good? What could be improved?). The second goal of the study was to answer questions regarding users' concern (e.g. what are the concerns regarding the usage of the application, if any? What are the obstacles that would hinder usage?)

With these questions in mind a storyboard concept test was designed. The participants of the study were presented with usage scenarios by the help of sketches. Those scenarios gave examples on the systems' functionality. The selected scenarios were an online-game scenario in which only users above the age of 18 could register, a discount scenario in which Egofy provided evidence that the user is eligible to receive a student discount while purchasing a train ticket, and a bonus point scenario where the (fictive) user redeemed gathered bonus points while making a transaction.

Summary of scenarios and their purpose

- Registration for the identity management platform and connection with attribute providers
- Registration for an online game (age verification)
- Buying a train ticket at the vending machine (student status verification and bonus points gathering)
- Car rental (efficient registration and bonus point redeeming)

The first sketch visualized how the registration for the system is done. It was emphasized that the system does not store any data, but that it acts as a broker between different trustworthy identity-providers (Cf. Figure 16). After the registration process, the scenarios were described.

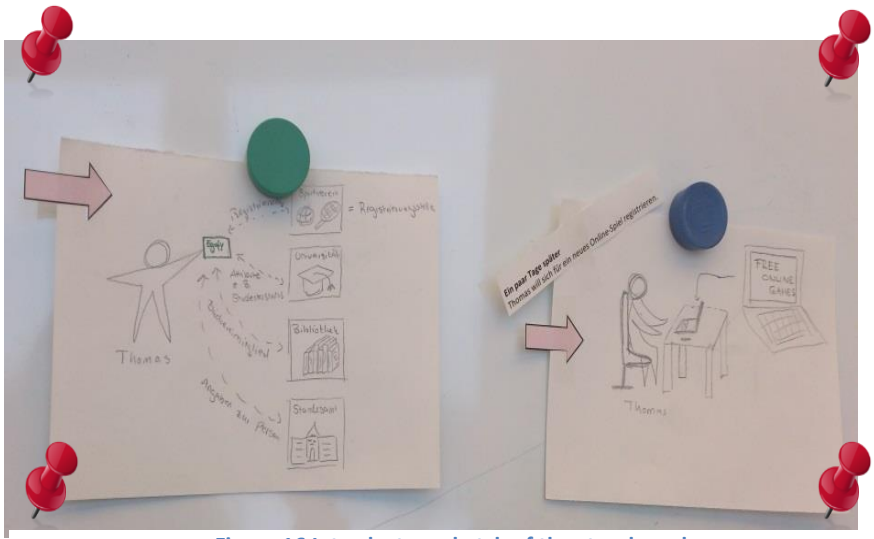

Figure 16 Introductory sketch of the storyboard

The study was supposed to have 75 minutes duration. At the beginning, participants had time to look at the storyboard as long as they wished in order to get an overview of the system. Afterwards, an interview was conducted. Participants were reimbursed with 12€.

The questions of the interview were:

- Could you please describe what you saw on the storyboard?
- What are your spontaneous impressions about this?
- What is Egofy?
- What can be done with Egofy?
- What do you really like about the application? Why?
- What do you really dislike about the application? Why?
- Could you imagine using the application? Why?
- Do you have any concerns regarding the usage of the application? Why?
- Do you see obstacles for using the application? Why?
- Could you think of any other scenarios where Egofy could be useful?
- Could we improve Egofy in any way?
- Do you think that your privacy is sufficiently protected by Egofy?
- Do you think that your data is sufficiently protected by Egofy?
- Would you trust Egofy? Why?
- Please rank the following answers according to your view:
    - In order to build trust in Egofy the provider of the application should be
        - A customer-oriented, local company
        - An international, world-wide operating enterprise
        - A state authority

Study 3: Participants:

11 potential users (6 male, 5 female) participated in the study. The participants were between 26 and 54 years old with an average age of 34 years. Different occupational groups were represented in the study among them 5 students, 3 self-employed, 1 retired, 1 employee, and 1 job seeker.

Study 3: Results

The participants appreciated different aspects of the system. The most important positive factor of the system showed to be efficiency, noted in different kind of aspects. Privacy and rewards seem to play a role as well; however, they were not mentioned as extensively as efficiency. An overview of the features which the participants liked is given in the following:

Efficiency

- That processes are facilitated
- That time can be saved (when using the system)
- That it renders processes uncomplicated and is comfortable in handling
- That there is only a single registration necessary to use the system
- That the system is usable spontaneously and independently of working hours
- That the system is an all-in-one solution with virtually unlimited capacity of attribute providers

Rewards

- That there is a possibility to gather bonus points

Privacy

- That every party within the systems only knows what is required to finish the business process

However, the participants were also concerned regarding different aspects of the system, such as misuse of the system, attacks and hacking, as well as non-transparent financing.

Misuse

- That their data might be abused (regardless of high privacy policies) either by third parties, or the identity provider or by abusing the token ("identity theft")
- That there might be a general tendency by involved parties to ask for more data than would be necessary to offer a service
- That sensitive data might be linked (regardless of mechanisms that should prevent it)

Attacks and Hacking

- That hacking might occur at the interfaces to the attribute providers
- Attacks/ hacking might occur during data transmission

Financing

- About how will the service be financed
- If the users' data might be used for (indirect) financing (e.g. through advertisings)?

Another interesting finding from the study is the trust enablers which were identified by the participants in the context of "Egofy". Three main groups of trust enablers were identified, whereas the most salient group was the "social factors".

Social factors

- Contact person to which questions can be addressed in the case of problems
- Positive experiences made by friends and other people from one's social network
- Positive reviews of other users or media
- Degree of establishment of the system
- Branding of the system provider

Technical and legal factors

- Reliability/ availability of the services

- Liability

Data protection factors

- Privacy policies/ Data protection measures
- Transparency about data processing

Study 3: Conclusion

Against our expectations, the privacy protection which is offered by the "Egofy" system was not the main benefit which the users perceived. Factors related to efficiency and rewards were named most often as a benefit.

Moreover, users raised many concerns regarding privacy, data protection and security, even though security and privacy are the fundamental pillars of the system. Different social factors, technological, legal and data protection factors were named as trust enablers.

The issue of the participants seeing mainly efficiency and monetary rewards as a benefit points towards the "secondary task problem". Thus, privacy and security might be rather seen as a hygiene factor, which raise concern when absent or not sufficiently visible and at the same time they do not contribute to a perceived increased benefit when present.

Study 4: Users' knowledge and feelings surrounding threats and mitigations on smartphones

In the second qualitative study users' knowledge and views of threats and strategies to mitigate these threats were explored. As a use case smartphone security and privacy was selected.

Exploratory studies serve the purpose to "investigate little understood phenomena, identify or discover important categories of meaning, and to generate hypotheses for further research" (Marshall & Rossman, 2010).

Even though the user research within Task 2.1 of ATTPS is framed within the basic concepts of usability, privacy, and trust, there is a need to further explore and uncover influencing factors for security and privacy related user behavior. This can help to better understand users' approaches to this topic and to advance the trust paradigm shift. Former work has shown that users feel concerned about smartphone threats (cf. e.g. Felt et al. , 2012 a; Chin et al., 2012; Ben-Asher et al., 2011), but so far there has been little work done into investigating which potential threats and mitigations of smartphone usage users actually know and how they perceive them.

Study 4: Design of the study

The design of the study follows a phenomenological approach which assumes that participants' knowledge is represented through conscious experience (Calder, 1977). Therefore, this approach can be also considered as experiential. Two focus group studies were conducted in which users discussed about the advantages, the disadvantages (potential threats) and the mitigations for those threats. A detailed overview of the study design is given in (Kraus et al., 2015).

There were four open questions which were discussed during the study by the participants:

- Which advantages do smartphones offer?
- Which disadvantages result from the advantages? (potential threats)
- How would you call the disadvantages? Are they threats, dangers, negative consequences or maybe something completely different? (wording question)
- What can users do to protect themselves from the disadvantages? (potential mitigations)

The study was designed to allow users to talk about their knowledge and opinions as open as possible without being biased by questions selected by the researchers.

Before the study was conducted a literature review of threats and mitigations related to smartphone security and privacy was done (Shabtai et al., 2009; Hogben & Dekker, 2010). The found threats and mitigations are given in Figure 17. The list served as a reference to

later on compare which of the threats and mitigations were named by the users during the study.

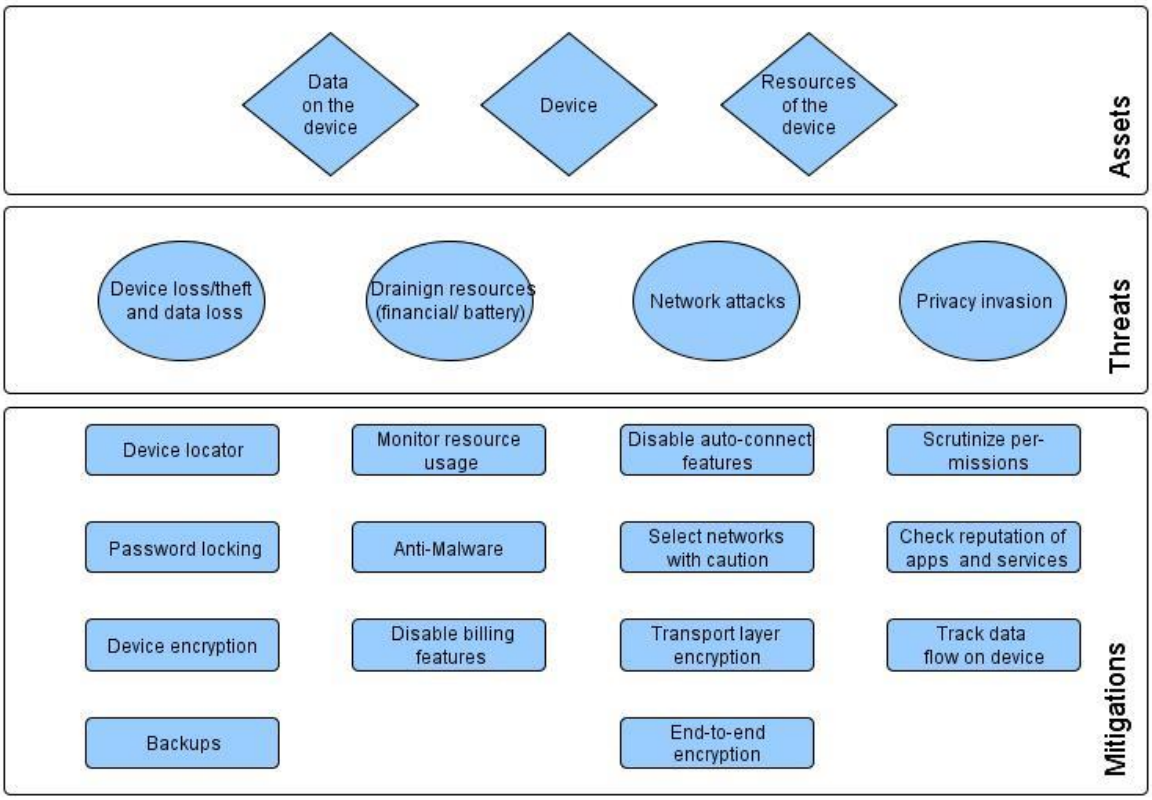

Figure 17 Threats and mitigations on smartphones

A detailed overview of the analysis procedure is given in (Kraus et al., 2015).

Study 4: Participants

Each focus group had six participants.

Focus group 1:

Four female and two male users participated in the first focus group. They were between 26-53 years old. Four participants were below the age of 35 and 2 were above the age of 35. None of the participants had a professional IT background. Half of the participants had a secondary school degree, while the other half had a university degree. Occupational groups of the participants were employees (2), self-employed (1), apprentice (1) and students (2). Five participants owned their smartphone for 1-3 years and one participant owned it longer than 3 years. There were 5 Android users and one Windows phone user in the group. Half of the participants reported using their smartphone several time per hour, while the other half reported to use it approximately once per hour. All participants

reported to download apps, either regularly or from time to time with one participant stating to download apps rarely.

Focus group 2:
Again, four female and two male users participated in the second focus group. They were between 20-58 years old. Half of the participants were below the age of 35. Half of the the participants had a professional IT background. One participant had a secondary school degree, two had a general qualification for university entrance, and three had a university degree. Occupational groups of the participants were employees (1), self-employed (1), housewife/stay-at-home-husband (1) and students (3). Two participants owned their smartphone for less than one year, two for 1-3 years and two participants owned it longer than 3 years. There were four Android users, one iPhone user and one Windows phone user in the group. One participant reported using the smartphone several times per hour; however, most of the other participants (4) reported using their smartphone several times per day, while one participant reported using it several times per week. Most participants (4) reported to rarely download apps, the other two participants reported to download apps 2-3 times per month or one time per month.

Study 4: Results

The focus group discussions revealed that already a small group of users was able to identify many of the threats and mitigations as in the smartphone risk management literature. Of course, this knowledge should be regarded as collective knowledge and we cannot draw assumptions on each participant's knowledge level nor generalize the results. However, as the study was of explorative nature we are interested in finding new ideas and opinions of users about smartphone threats and mitigations. Besides the knowledge, we also find that users' views on potential threats and mitigations are influenced by negative feelings such as social pressure, helplessness, dependency and fatalism. In the following these feelings will be described by quotations made by the participants.

Peer pressure:

FG1-P2: "This means that even if you wanted to totally boycott the system [i.e. for instance the way privacy is handled], one does not have a choice."

"Social" availability" refers to expectations regarding the availability of the smartphone user or the feeling of being monitored by others:

FG1-P1: "It's being expected that you are available at all times."

FG2-P4: "Constant availability."

FG1-P4: "Like surveillance. So if the others [colleagues] definitely saw that one's been online, I can't tell my boss 'Oh, I'm sorry I didn't see that you wanted me to help out.' "

FG1-P5: "Mistakes could have been made by everybody, but nowadays it's so obvious. Mistakes are getting immediately discovered."

Harassment by advertiser:

FG2-P5: "[...] they later said: We will call you until you take part in the survey."

FG1-P1: "[...] and occasionally they render the whole website as an ad. [...]Therefore, you don't have the chance to continue on what you wanted to do, but you need to give attention to the whole thing. [...] "

Dwindling trust in the system in security aspects and respecting privacy:

FG1-P3: "It was always getting worse, that really every app wanted to access everything. So, four years ago, the first apps [...] weren't like this that they wanted to know everything."

FG1-P2: "Well, when it comes to emails, in the past one could get an e-mail address for oneself and nobody knew to whom this address belonged to. But if you nowadays retrieve your emails on your mobile you are immediately identifiable."

Trust as a mitigation refers to trust in the smartphone OS or the service provider as an effective action to mitigate threats:

FG1-P3: "[...], so, the provider is just crucial."

FG1-P3: "[...] with their cloud [storage service] there's at least more security as their company is based in Germany."

FG1-P1: "As far as I know Windows is more secure."

FG1-P1: "Exactly, I know, these WLAN networks that I do not trust, I should delete them [...]"

Dependency on third parties describes a feeling of dependency as one has to rely on third parties and their decisions regarding security and privacy:

FG1-P2: "That is the thing, I am dependent again on someone and I again do not know, how safe this really is, that is again another alleged security, which leads me to dependence." [On the topic of encryption]

FG1-P4: "So, this is quite stupid in the app market, that only if you are on the most up-to-date level, you get access to the apps, and that's why you get forced to always renew everything."

Psychological dependency refers to the feeling of being dependent on the smartphone:

FG2-P3: "Dependence. Well, you really make yourself dependent if you rely on this device."

FG2-P4: "Bad is also this psychological pressure, so to say, that one would be missing out on something."

Helplessness

FG1-P2: "But the worst thing nowadays is that for some things it's not our fault, for example if we visit some webpages, everything is recorded."

FG2-P3: "Yes, exactly, that there is data, umh, traffic which you are not so... aware of."

FG2-P4: "But that's, I think, the same as with your apartment's front door. You can lock it with ten locks or just with one, but if one wants to get in, so to speak, one will get in." [On the topic of encryption]

Fatalism

FG2-P2: "None, really no communication option with the mobile is secure. Not a single one."

FG2-P2: "There's nothing you can do against it."

FG1-P5: "You have to take into account that everything [...] can be hacked by somebody at any time or can be available somehow and spread through the internet. Nothing is secure, thus."

Sacrifice security for usage refers to a feeling of having no choice:

FG1-P2: "[...] because of everything already that I am googling, every single word that I type is recorded, every single website that I looked at, every single text that I looked at, all my data that is on my phone, especially these authorizations of these apps, if I agreed to something somewhere, where I HAD TO, so that I am allowed to use the application."

FG1-P1: "[...] it is seen by many [people] like this, that it [the disadvantage] is something that you have to accept [...]"

Exercise one's own influence by informing oneself refers to a feeling of being capable to handle security issues by applying actions which one is capable to do (e.g. informing oneself):

FG1-P4: "I just may pick this up again, it is really like this, if one is not informing oneself, it's one's own fault."

FG1-P1: "So, there are certain things I can protect myself against, against others I cannot. Partly because I do not really know what are all things that can happen. And that is the key... So ... we need a kind of responsibility, enlightenment, information.... I think, that is missing a lot."

Exercising one's one influence refers to a feeling of being capable to handle security issues by applying actions which one is capable to do (e.g. by controlled disclosure or individual responsibility)

FG1-P4: "[One should not upload pictures] That's obvious. I never post any pictures of me on the internet,... "

FG1-P3: "[...] Well, let me say, one has got minimal influence on what one discloses. One really needs to read further into the topic [...]"

FG2-P3: "One can circumvent everything [all disadvantages] if decisions are made consciously and if one makes oneself clear: what could happen? Do I want this? Or do I not want this?"

FG2-P5: "One certainly needs to reflect, whether this is what one wants or what one doesn't want [...]"

The negative feelings described above relate either to the usage of security mechanisms or smartphone usage in general. Thus, depending on the context, they can be either seen as an opportunity or as an obstacle for the adoption of security mechanisms and trustworthy ICT. Negative feelings related to smartphone usage in general, such as peer pressure, can be mitigated by security and privacy by design and default: for instance this way the users do not need to choose between their primary task (staying connected with their friends) and security (do this in a secure way). Also, issues such as “social” availability can be mitigated by privacy settings in apps which offer social interaction.

The negative feelings were interpreted as being antonyms of basic psychological needs such as autonomy (e.g. antonym = dependence) and competence (e.g. antonym = helplessness). **Therefore, the subsequent interviews investigate the topic of intrinsic motivation related to psychological need fulfillment.** The purpose of this is to determine whether it makes sense to include basic psychological needs and motivational aspects in the survey design.

Another issue which was found in the study was unmerited trust. Users may be led in some cases by misconceptions regarding security and privacy. Trust might be used as a shortcut for security and privacy without verifying the actual extent of these features. User education and awareness might help to mitigate this threat.

Study 5 & 6: Users' motivation to apply security and privacy actions on smartphones

Whereas the focus group studies aimed at exploring end-users' knowledge and views on security and privacy on smartphones, a second study in form of individual interviews was conducted to explore what users actually do to protect their security and privacy and what motivates them to do so. Basic psychological needs were used to classify groups of motives. The interview study was further extended by an online study in which the need questionnaire as described in Section "Measuring factors for intrinsic motivation" was employed.

Study 5: Interviews

The semi-structured in-depth interviews were centered on the following research questions:

- Which security and privacy actions are done by smartphone users? (What)
- How are they done? (How)
- Why are they done? (Why)

Psychological needs can be found in the "why" plane (cf. Hassenzahl, 2010). Therefore, we considered the why questions to provide answers to the reasons and annotated them with the psychological needs (if applicable).

A detailed description of the interview procedure and analysis can be found in Kraus et al. (2016)[9].

Study 5: Interview Participants

Demographics: 19 smartphone users (10 female) were recruited from a panel of our institution. The age ranged from 18 to 58 years with an average of 31 years. Participants had diverse school degrees (approximately equally distributed among secondary school degree, qualification for university entrance, and university degree). Among the sample were 9 employees, 7 students and 3 job seekers.

Smartphone Usage: There were 13 Android users, 5 iPhone users and 1 Windows Phone user. Smartphone usage experience among participants was diverse: 4 participants had owned their smartphone less than a year, 7 for 1-3 years and 8 for more than 3 years. Most of the participants use their smartphone at least once per hour (N=15). Only one participant had a professional IT background.

[9] Conference paper submitted for review; Deliverable will be updated as soon as the publication is accepted

Study 5: Interview Results

The results from the interview study suggest that a variety of psychological needs (i.e. motives) drive security and privacy actions on smartphones.

A few examples are given in the following.

Concerning the **purchase of the smartphone** for instance Money/Luxury and Relatedness were found as motives.

Money/Luxury:

"It [the smartphone] was the cheapest" (P5)

"[The decision for the operating system was] a conscious decision, but not conscious for Android but rather […] conscious for the price. Otherwise it would have been an Apple."

Relatedness:

"[…] to be in contact with my friends by using Whatsapp or so that was the main reason [for buying a smartphone]." (P12)

Security and Keeping the meaningful were found as motives related to **making backups**.

Security:

"Yes, because the data on my mobile phone is important to me… and well it is better… safety comes first" (P8)

Keeping the meaningful:

"It happened once that I dropped my phone […] and afterwards all the data was gone […] And there were many pictures on it, many funny videos and everything… then I thought to myself: 'that shouldn't happen again'". (P12)

A detailed overview and analysis of the results can be found in Kraus et al. (2016).

Study 6: Online Study

We conducted an online survey to find further evidence for these results and to determine in more detail which actions are driven by which needs. Within the survey we deployed the need questionnaire provided in Sheldon et al. (2001).

The participants were asked whether they deploy certain security and privacy actions: installing updates, protection from theft, password locking, scrutinizing permissions, checking the monthly bill/ prepaid balance, doing backups, managing data connections (WiFi, Bluetooth, GPS), privacy settings of messaging apps, and using messaging apps with end-to-end encryption.

If the participants indicated that they perform an action, they were given the need questionnaire with the introductory sentence "By doing [action] I have the feeling that…". If they indicated that they do not perform an action, the introductory sentence was "By not doing [action] I have the feeling that…". As the need questionnaire had to be answered for

each security and privacy action, the survey was split into three parts to avoid possible fatigue effects. Thus, each participant was asked for three security and privacy actions and not for all nine of them. To further reduce possible fatigue effects, participants were only given 2 of the 3 items of the original need questionnaires.

A detailed description of the online study procedure, analysis and results can be found in Kraus et al. (2016).

Study 6: Online Study Participants

70 participants took part in the study, 24 of them received version 1 of the questionnaire, 23 version 2, and 23 version 3. Participants were between 18 and 61 years old with an average age of 28.08 years. The sample was diverse smartphone usage, frequency of usage, and occupational groups; however, there was a bias towards male participants, higher educational levels and undergraduate students.

Study 6: Results

The results of the online study suggest that for some security and privacy actions on smartphones certain needs are more salient than others (e.g. “Keeping the meaningful” for backups, “Stimulation” for updates, and “Autonomy and Competence” for permissions). Other actions (e.g. passwords) are associated with low need fulfillment. The need questionnaire showed to be applicable and to deliver significant results in the context of smartphone security and privacy actions. Please refer to Kraus et al. (2016) for detailed results and statistical analysis.

Conclusion of all conducted user studies

Whereas the quantitative user studies covered mainly usability issues and the influence on different variables on user behavior, the qualitative studies revealed new insights into the feelings, needs and motives which are associated with the usage or non-usage of trustworthy ICT. Those insights offer new opportunities for usable and UX oriented design of trustworthy ICT, as well as opportunities for higher user satisfaction and thus for increasing the potential to advance the trust paradigm shift (cf. Section 5). The survey design provides an overview of questionnaires which can be used in this context.

4. Mobile payment reference design

In the following a reference design for trustworthy and usable security for a mobile payment system is presented. The results which led to the reference design are based on several experiments which were conducted to evaluate a mobile payment system regarding users' perception of security and usability. The evaluation was based on an NFC-based mobile payment system prototype. The experiments aimed to discover general relationships between user characteristics (e.g. risk perception, personality), perceived security and risk, and usability.

Scope:

The reference design is focused on usability and security issues related to the users' perception of a mobile payment system. It does not cover security aspects related to the actual security of the device and its components. These aspects depend on the platform upon which the mobile payment application is built. Some of those aspects are also addressed in the generic trust architecture of ATTPS (cf. Deliverable 3.1).

Principles of Mobile Payment

There is a lack of a clear definition of what mobile payment is. For instance, mobile payment can be defined as payment transactions which are made by the help of a mobile phone or smartphone. For the reference design, we consider mobile payment as "the task of making generic point-of-sale (POS) based payments using a smartphone" (Sieger, 2015). During the last years mobile payment has spread as an additional method for making POS transactions. For instance, in the US, systems like Apple Pay, Google Wallet and the Starbucks App appeared on the market; in Germany BASE Wallet, Smartpass and MyWallet evolved; Apple Pay was also brought to market in the UK; and in Korea and Japan, systems like Samsung Pay and Sony's Felica, respectively, are available. M-Pesa is in widespread use in Kenia.

These available systems all use different underlying technology. While they may use NFC as a means of exchanging data at the point of sale, they are not necessarily interchangeable. For example, you cannot use Apple Pay in Tokyo's public transport, although the Felica system is NFC-based as Apple Pay is. Starbuck's mobile payment app uses QR codes and is thus a closed-looped system to be used at Starbuck's only.

Also, a mobile payment system app is dependent on the hardware and the operating system (OS) as shown in Figure 18. Especially third-party app developers depend on the platform upon which they build their app, also with respect to the implemented security methods (Sieger, 2015). For instance, if near field communication (NFC) is not integrated into the device there is no possibility to make NFC-based payments; likewise, if the device does not feature biometric identification methods, they cannot be implemented. On the other hand, the app is also dependent on the security of the hardware, the OS and the APIs. The security aspects within the mobile payment reference design focus on the security which is

perceivable by the user – e.g. the authentication method of the app or the requested permissions.

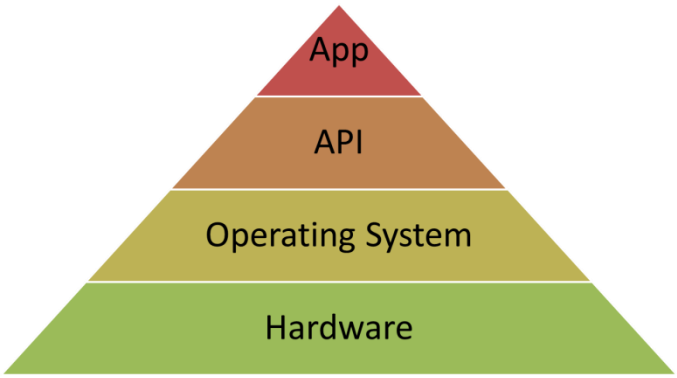

Figure 18 Schematic overview of the relationship between Hardware, operating system, API and (mobile payment) app.

App design

The mobile payment system design depends on the requirements which were provided by the customer. Besides these requirements, there exist different "general" paradigms which can serve as a basis for the mobile payment system design (cf. Figure 19). Therefore, the mobile payment app can be designed according to (at least) three different paradigms.

Using the app paradigm each use case (payment, loyalty card, coupons etc.) is contained within a single-purpose app. Any overlapping use (e.g. redeeming coupons while paying) is done by exchanging information across the apps using a common API provided by an underlying mobile payment system.

The object-based (or card-based) paradigm uses a visual presentation of the payment card(s) (plus loyalty cards and coupons) to ease the transformation from a physical object (the plastic cards and paper coupons) to a virtual one. The mobile payment app usually contains all use cases in one app. In the prototype upon which the empirical experiments are based, the card paradigm was deployed.

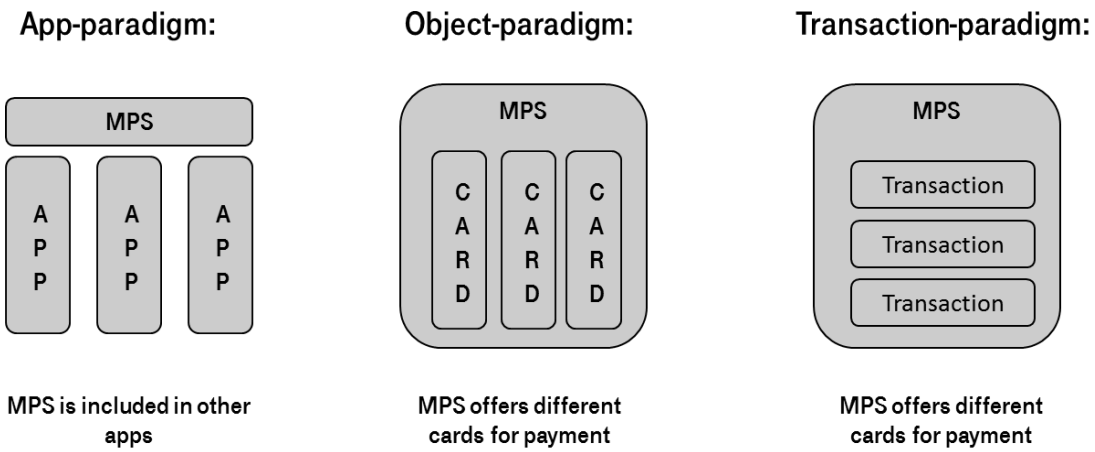

Figure 19 Examples for mobile payment app design paradigms

The transaction-based paradigm gets completely rid of any visual cues to the physical objects and focuses on providing data on transactions. It also may add additional visualisation of the data, for example, pie charts for transaction categories (food, entertainment etc.).

App ecosystem

The ecosystem surrounding a mobile payment app based on the card paradigm is depicted in Figure 20.

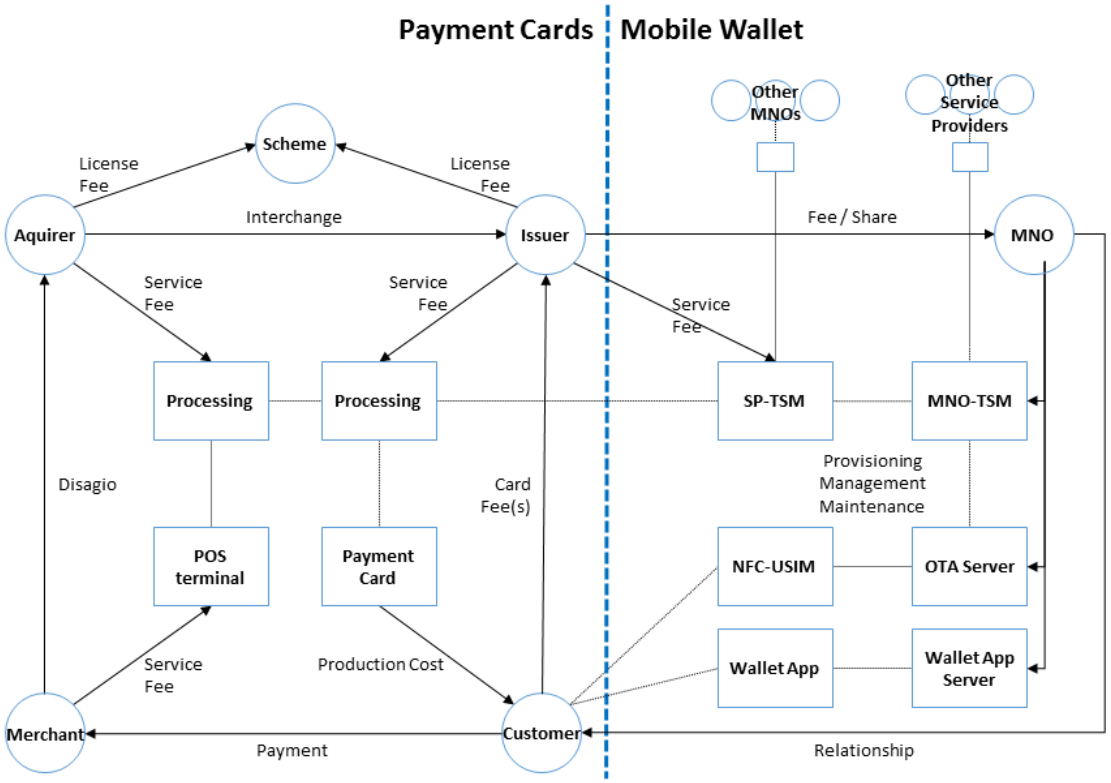

Figure 20 Mobile payment ecosystem (graphic by courtesy of Hanul Sieger)

For the card-based transaction, a point of sale (POS) terminal is required which connects to a payment processing network via telephone line (landline or mobile) or through an IP-based network. Transactions can be either “card-present" or “card-not-present". Whereas the first refers to a situation where the merchant can see the card, the latter refers to a situation where the card cannot be seen by the merchant (for instance when mobile payment is used). There are different methods how a transaction is processed. It may be batch-processed, when the (cash) register is closed, e.g. when a shops closes in the evening. Or it may be processed in real-time.

App Security

The security of a mobile payment app depends, as described above, not only on the security methods of the app itself, but also on the security approach of the smartphone hardware, the operating system, and the APIs. For instance, the hardware can contain a secure element as suggested by AMS and STMicroelectronics in their hardware reference design[10]. Most smartphones feature a sandbox approach concerning operating system security. Each application thereby runs in a sandbox environment. Thus, for instance, Android[11] and iOS apps share resources for which apps must request permissions. The critical permissions are shown to the user either during the installation process of an app (Android) or when the app requests the permission for the first time (iOS). This is therefore also a security feature which is perceived by the user (cf. also Section 4.3), but its presentation depends on the smartphone platform, i.e. the operating system. As mentioned above, the mobile payment reference design presented in this section focuses on the app itself and the security features of the app such as the authentication method used within the app (independently of hardware, operating system and API security).

Mobile Payment Prototype

The mobile payment app which served as an artefact in the studies was designed according to the object/card paradigm. Different cards which relate to actually existing cards of the user are presented within the app and the user can choose which card should be used for the transaction. The app was an Android mock-up application called “Mobile Wallet” on a NFC capable Android smartphone. The application had the following features: payment, travel tickets, event tickets, access (e.g. opening doors), and customer loyalty cards. The application itself can be used with authentication methods such as PIN or fingerprint recognition.

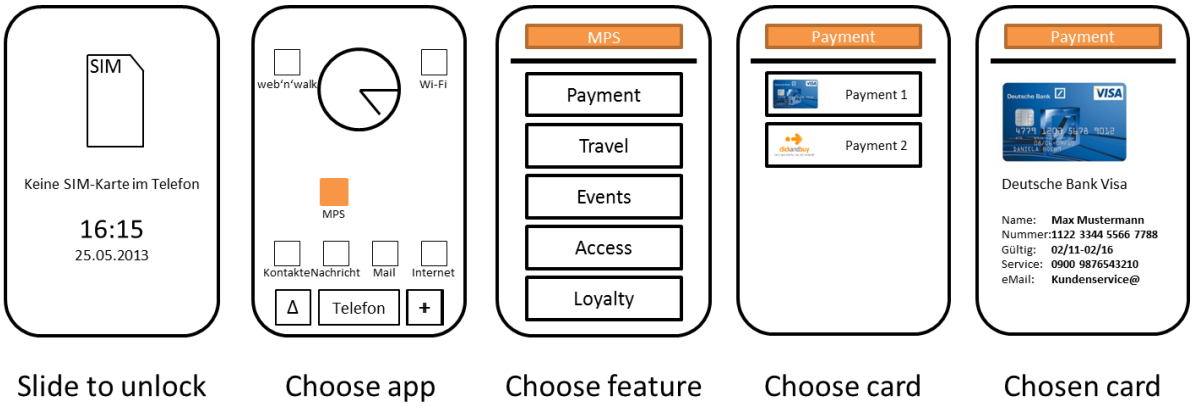

Figure 21 Schematic overview of interaction for the payment process used in the studies

[10] http://www.nfcworld.com/2015/02/26/334302/chip-makers-ams-and-st-team-up-for-wearable-nfc-payments/

[11] http://developer.android.com/training/articles/security-tips.html

Figure 21 shows the simplified screens seen by the user during the payment process when neither PIN nor fingerprint recognition is used for authentication. After selecting a card, the user has to hold the phone near the POS NFC reader to conclude the transaction.

Study Design

Five experiments were conducted from 2010 to 2013. The studies were conducted in a laboratory setting with several shops, where test users had to buy different goods under varied conditions. The tests were designed around three main parts:

- Users' intrinsic characteristic (personality traits ("BIG Five"); technical affinity; risk behavior and perception); The data concerning these factors was collected using standard and self-developed questionnaires. The standard questionnaires consisted of "BIG Five" (Gerlitz & Schupp, 2005), which are the dimensions of human personality described by five factors (openness, conscientiousness, extraversion, agreeableness, and neuroticism. Risk perception and risk behaviour was measured with "Domain-Specific Risk-Taking DOSPERT-G" (Johnson et al., 2004). In order to detail technology-related personality traits the questionnaire "Technische Affnität Elektronische Geräte (TA-EG)" was used (Bruder et al., 2009). A self-developed questionnaire was used for demographical data and asked for knowledge and experience related to computers and smartphones.
- System characteristics (with questionnaires on use and perception of mobile payment and the app itself); The perception of the usability of the mobile payment application was measured using "System Usability Scale SUS" (Brooke, 1996), and the user experience, especially hedonic and pragmatic qualitiy, using "AttrakDiff" (Hassenzahl & Monk, 2010); and user behaviour (the test of the payment app); Perceived security and perceived risk was measured using a short self-developed questionnaire.
- The different test runs varied; There were modifications of the self-developed questionnaires; variation of the shop setup; different security methods (none, PIN, fingerprint), and security threats ("attacks"):
    - Study 1: fully functionalized setting of the prototype, interview-like shopping sequence, 1 participant per run, 12 participants in total
    - Study 2: four shops, no security method and attacks, 1 participant per run, 20 participants in total
    - Study 3: four shops, with and without PIN, with and without attacks, two participants per run, 17 participants in total
    - Study 4: two shops, with PIN and attacks, 1 participant per run, 20 participants in total
    - Study 5: two shops, with fingerprint and attacks, 1 participant per run, 19 participants in total

Figure 22 depicts the factors related to the mobile payment app and its user interface that were investigated in the experiments. Factors in grey were not considered. Figure 23 depicts the usability, UX and usage factors that are considered in the mobile payment reference design.

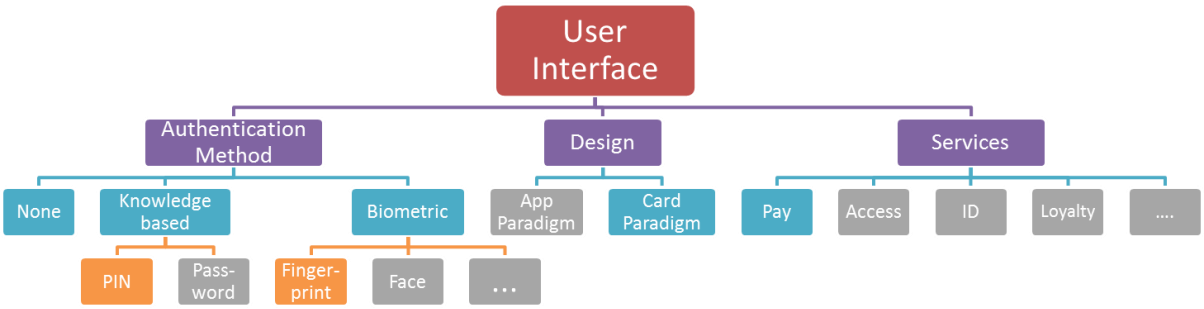

Figure 22 App factors considered in the mobile payment reference design

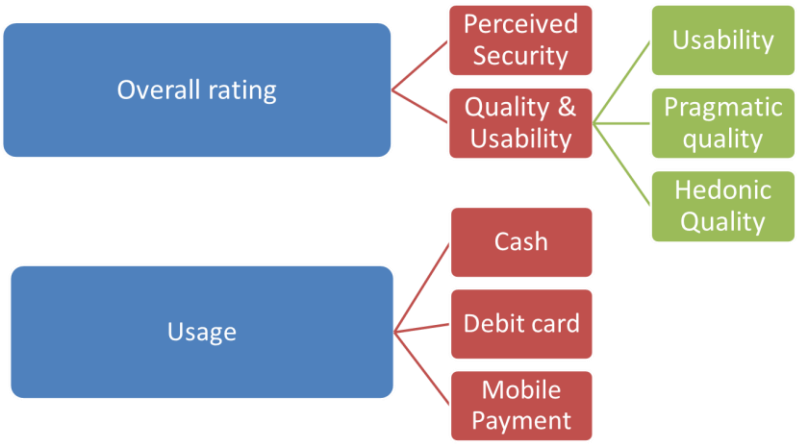

Figure 23 Users ratings and usage factors considered in the mobile payment reference design

The reference design described hereafter is based on lab studies which have been conducted between 2010 and 2013. The lab studies were designed to appear as realistic as possible to the user (Sieger et al., 2012). By the time the studies were conducted there was no mobile payment solution available on the market in Germany. However, even if a mobile payment solution would have been available on the market, the feasibility of a field study with a focus on security is questionable. First, as depicted in Figure 20, there are many stakeholders involved in the mobile payment process. Bringing all of them together on a

table in order to conduct a field study would be an effortful endeavour. Second, ethical considerations are likely to inhibit a mobile payment field study with a focus on security, especially in the presence of (simulated) threats.

Results of the mobile payment system user studies

In the following the results of the experiments are summarized. Please refer to (Sieger, 2015) for details.

The influence of the authentication method on quality and usability ratings

The experiments show that if an authentication method is applied, perceived security was rated higher. Thus, having an authentication method contributes to a higher perceived security. However, when a PIN was deployed, the participants also used mobile payment less often compared to no authentication method and fingerprint. There was no difference in usage frequency between fingerprint and no authentication method.

Usability ratings on the SUS scale ranged between good and excellent. For AttrakDiff, pragmatic quality (which can be considered to be closely related to usability) and attractiveness did not show to be influenced by the authentication method.

Regarding hedonic quality, PIN and Fingerprint were rated higher compared to the prototype without authentication method. Thus, having a security method increased the hedonic ratings of the prototype.

Table 10 provides the tendencies regarding perceived security, hedonic quality and usage by authentication method that have been found in the user studies.

Authentication Method	Perceived Security	Hedonic Quality	Usage
None	↓	↓	↑
PIN	↑	↑	↓
Fingerprint	↑	↑	↑

Table 10 tendencies of perceived security, hedonic quality and usage by authentication method

Personality factors, technical affinity, experience, and risk perception

Regarding personality factors, it was found that participants with a high degree of agreeableness (“being sympathetic and cooperative”) rated overall perceived security lower if **no security method** was present in the prototype. Moreover, they overall used mobile payment less often.

When a PIN was applied as authentication method, the overall usage of mobile payment was moderate positively correlated with the overall use of mobile payment for participants

that scored high on conscientiousness. In the cases were “attacks” were applied within the experiment, the correlation vanished for those participants.

When fingerprint was applied as authentication method, the overall usage of mobile payment was positively correlated with the overall use of mobile payment for participants who scored high on openness .

The personality traits neuroticism and extraversion did not show to have an influence on behaviour and security ratings.

Regarding technical affinity, the construct of “positive attitude towards technology” showed to have a positive influence on mobile payment usage and perceived security ratings.

Also, participants who scored higher on the believe that their phone is in danger despite using a PIN, rated perceived security lower when PIN was applied as authentication method. However, participants who already use a screen lock with PIN on their mobile phone rated perceived security higher.

User characteristics of risk perception and behaviour were inconclusive regarding their relation to the rating and usage of the system.

Mobile Payment Reference Design for Usability and Security

The findings from the studies suggest the following for a mobile payment reference design which is based on a card paradigm.

If the designer is interested in a high usage frequency, a high perceived security and high hedonic quality ratings, a “new” authentication method such as fingerprint should be employed as this method showed to score high on all three factors. Still, it should be investigated in future studies whether the high ratings for hedonic quality and the high frequency of usage relate to fingerprint specifically or if any new security method which has a sufficient usability is likely to increase usage and hedonic quality. Security perception was for both, PIN and Fingerprint, higher compared to no authentication method. However, deploying a PIN is likely to decrease the usage of the payment system, even though security perception is better compared to no authentication method.

The results which we found are based on a system that received high usability ratings independently from the authentication method. Therefore, high usability is a prerequisite for the system: besides selecting an appropriate authentication method, the system should be iteratively tested for usability during its design.

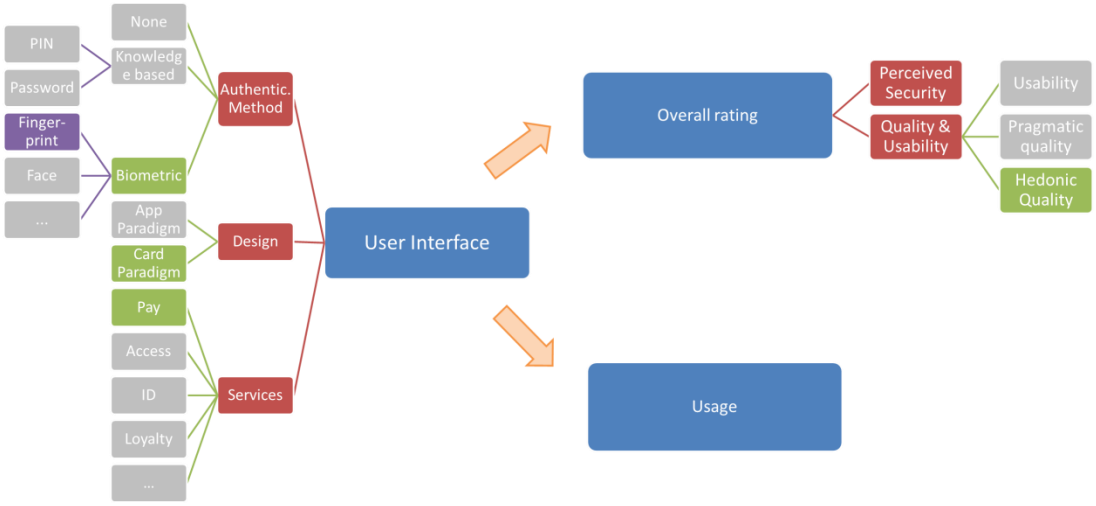

Figure 24 Mobile Payment Reference Design: relation between user interface factors, user ratings and usage.

5. Lessons learned

In this Section we summarize the lessons learned during this project. In the appendix screenshots of a running dashboard tool prototype is provided. The dashboard tool is meant to aid software architects and programmers to design usable and secure applications.

The work on the survey design and the discussion during the ATTPS meetings led us to the following conclusion.

Usability is an important aspect of the design of security and privacy solutions. Much effort has been spent during the last years to investigate usable security and privacy (cf. e.g. (Cranor & Garfinkel, 2005), (Garfinkel & Lipford, 2014)). However, the user behavior depends also on use situations, intrinsic motivation, and the users' primary goal. Within Task 2.1 of ATTPS, several questionnaires have been deployed in a survey design and the influence of the constructs which were measured with those questionnaires has been further investigated. Moreover, qualitative studies and mixed method studies (i.e. studies that combine quantitative and qualitative methods, cf. Section 4, Study 5 and 6) targeting user experience issues have been conducted to further explore use situations and the influence of a user's primary goal and motivation on the interaction with security and privacy applications.

Security and privacy solution architects might now pose the following questions:
When is it useful to apply usability engineering methods and when is it useful to apply experiential methods? In which situations should both methods be employed? When do user characteristics influence user behavior and if so, what kind of behavior?

From the experience gained in this project we suggest to distinguish between two kinds of situations.

Situation 1: Security and privacy are not visible to the end-users
The first situation is the one when security and privacy solutions are not visible to the user. The reason for this can be for example that those solutions are implemented in the backend of a service or application or that those solutions do not require an interaction with the user. An example for the former would be the backend of a privacy enhanced federated identity management system (as in the "Egofy" system considered in Study 2). An example for the latter would be messaging apps on smartphones that deploy end-to-end encryption. Public key exchange in this kind of applications is for example done via a key server where the public key which belongs to a user is automatically identified by the help of the user's phone number and automatically mapped to contacts in the user's contact list.

Regarding the design of trustworthy ICT we recommend to address the understanding of user behavior in this kind of situation (i.e. when security and privacy protection is not visible to the user) by employing experiential approaches to empirically investigate the issue. Thereby one could learn about primary goals of the users, use situation and motivation which yields understanding on why trustworthy solutions are used or not. Based on this

knowledge actions can be taken to adapt trustworthy ICT to use situations and increase users' intrinsic motivation to use them. Also, as a prerequisite, usability engineering methods should be applied to ensure a high usability of the product.

Another important aspect which has become visible during the project is that in those situations where security and privacy are not visible to the user "trust" comes into the picture: In both examples mentioned above the user needs to trust the service provider that the security and privacy technologies and procedures are implemented correctly and not corrupted. This is, on the one hand good, as it removes the burden to get familiar with complex technical procedures from the user and reduces the additional effort a user has to spend to interact with the system. On the other hand, this may also support unmerited trust, as the user might not be able to distinguish between trustworthy and untrustworthy service providers. This leads to the question of what makes a service or product provider trustworthy.

To this end, we see a huge potential for TDL to further advance the trust topic with respect to end-users.
First, TDL, as a consortium of international trustworthy ICT providers has already built a community of stakeholders interested in pushing the trust topic. This increases the synergies among consortium partners for building trust together.
Second TDL has a huge potential to define what makes trustworthy ICT "trustworthy", i.e. what makes services and products trustworthy, and how this can be communicated to the user. The generic trust architecture developed in ATTPS is an important step towards this goal. To communicate this to consumers, discussion among stakeholders are needed to design visible cues such as for example a "trust seal".

This is also where the question of "awareness" comes into the picture. The importance which a user assigns to the trustworthiness of a product or service is likely to depend on the degree to which the user is aware what trustworthiness means.

Situation 2: Security and privacy are visible to the end-users. End users are required to interact with security and privacy applications.
The second kind of situation is the one when security and privacy solutions are visible to the user, and the user is supposed to interact with them. The security system does then put an additional burden to the user in terms of time and effort. An example for this is authentication. This is the "classical" situation where it is crucial to apply usability engineering methods. To detail all of usability engineering methods would go beyond the scope of this project. However, Garfinkel and Lipfort (2014) summarize several lessons which have been learned during the almost two decades of usable privacy and security research: The number of decisions to be made by the user should be kept low, safe and secure defaults should be employed, a clear context and good information (clearly presented) should be provided to the user, and education works to a certain degree (Garfinkel & Lipford, 2014).

Besides applying appropriate usability engineering methods, experiential approaches can help in this situation to further understand users' interests related to the usage of the product. Moreover, experiential approaches can be a source of new ideas on how to improve user acceptance and user satisfaction with those security and privacy solutions.

Intrinsic user characteristics:
When it comes to intrinsic user characteristics, we have found privacy concern and privacy and security knowledge to have an influence on adoption (in the context of mobile security and privacy). For the AppChoice study (Study 2), no influence of intrinsic characteristics was found. Thus, the results suggest that intrinsic factors should be taken into account in studies on trustworthy ICT adoption rather than in lab experiments.

Recommendation to the TDL community

1. **Usability and User experience:** Additionally to usability engineering methods, methods from user experience should be deployed in the domain of trustworthy ICT. Further research is needed to determine whether improved user experience of trustworthy ICT products can advance the trust paradigm shift.
2. **Visibility of trustworthiness and unmerited trust:** It needs to be ensured that trustworthy ICT and the perception of trust are in line. The generic trust architecture defined components of a trustworthy system and is a first step towards this goal. A method for informing the user of the use of trustworthy components within products could be a "trust seal" for products and services which deploy trustworthy ICT component. Designing such a "trust seal" which can be easily understood by the end-users is a complex matter. Stakeholder discussions and user studies are needed to develop design ideas and to test those ideas in the field.
3. **Awareness:** It is desirable that trustworthy ICT can be easily used by users of different knowledge levels. In any case awareness that trustworthy ICT solutions are on the market is a prerequisite for adoption. Regarding the awareness raising, distinctions should be made between raising awareness on threats which can be mitigated through trustworthy ICT and awareness on trustworthy ICT and its deployment. Whereas threat awareness might rather increase privacy and/or security concern, awareness and education on trustworthy ICT and its deployment empower the users to take actions. Therefore, the focus of awareness raising should target both issues.
4. **Long-term effects:** Long-term effects on end-users' acceptance and adoption of trustworthy ICT induced by the given recommendations should be monitored.

6. Bibliography

4 safety tips for using Wi-Fi. (2014, 05. 26). Retrieved from Microsoft Safety and Security Center: http://www.microsoft.com/en-gb/security/online-privacy/public-wireless.aspx

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42(12)*, 40-46.

Bargas-Avila, J. A., & Hornbæk, K. (2011). Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2689-2698). ACM.

Ben-Asher, N. (2011). Modeling the Tradeoffs between Usability and Security in Information Systems. Doctoral dissertation, Ben-Gurion University of the Negev.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011). On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 465-473). ACM.

Bødker, S., Mathiasen, N., & Petersen, M. G. (2012). Modeling is not the answer! Designing for Usable Security. *interactions*, 54-57.

Brooke, J. (1996). SUS-A quick and dirty usability scale. *Usability evaluation in industry*, pp. 189-194.

Bruder, C., Clemens, C., Glaser, C., & Karrer-Gauß, K. (2009). TA-EG - Fragebogen zur Erfassung von Technikaffinität. Technical report, FG Mensch-Maschine Systeme TU Berlin.

Caballero, A., Kluitmann, M., & Berkley, R. (2014). *Deliverable 1.2 - Impact Assessment.* ATTPS Project.

Calder, B. J. (1977). Focus groups and the nature of qualitative marketing. *Journal of Marketing research*, 353–364.

Chellapa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 358-368.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 1). ACM.

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use.* O'Reilly Media, Inc.

Data Privacy Day. (2014, 05. 26). Retrieved from http://www.staysafeonline.org/data-privacy-day/privacy-tips/mobile

DeWitt, A. J., & Kuljis, J. (2006). Aligning usability and security: a usability study of Polaris. *Proceedings of the second symposium on Usable privacy and security* (pp. 1-7). ACM.

DoW. (2012). ATTPS Description of Work.

Dunphy, P., Vines, J., Coles-Kemp, L., Clarke, R., Vlachokyriakos, V., Wright, P., et al. (2014). Understanding the Experience-Centeredness of Privacy and Security Technologies. *Proceedings of the 2014 workshop on New Security Paradigms Workshop (NSPW)*, (pp. 83-94).

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). ACM.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. *The Economics of Information Security and Privacy*, 211-236.

Felt, A. P., Egelman, S., & Wagner, D. (2012 a). I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 33-44). ACM.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012 b). Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 3). ACM.

Fronemann, N., & Peissner, M. (2014). User experience concept exploration: user needs as a source for innovationl. *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundationa*, (pp. 727-736).

Garfinkel, S., & Lipford, H. R. (2014). *Usable Security: History, Themes, and Challenges.* Synthesis Lectures on Information Security, Privacy, and Trust, 5(2).

Gerlitz, J.-Y., & Schupp, J. (2005). Zur Erhebung der Big-Five-basierten Persnlichkeitsmerkmale im SOEP. *DIW Research Notes, 4*.

Gross, J. B., & Rosson, M. B. (2005). Looking for trouble: understanding end-user security management. *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (p. 10). ACM.

Hassenzahl, M. (2010). Experience design: Technology for all the right reasons. *Synthesis Lectures on Human-Centered Informatics, 3(1)*, 1-95.

Hassenzahl, M., & Monk, A. (2010). The inference of perceived usability from beauty. *Human–Computer Interaction, 25(3)*, 235-260.

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, affect, and interactive products–Facets of user experience. *Interacting with computers, 22(5)*, 353-362.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.

Hogben, G., & Dekker, M. (2010). *Smartphones: Information security risks, opportunities and recommendations for users. .* European Network and Information Security Agency, 710(01).

How to Make Smart Wireless Choices and Avoid Problems. (2012). Retrieved 26.05.2014, from Consumer Action: http://www.consumer-action.org/english/articles/cell_phone_ savvy_training_manual/#protect-info

Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy: An economic model for pricing personal information.* ENISA.

Johnson, J., Wilke, A., & Weber, E. (2004). Beyond a trait view of risk taking: A domain-specific scale measuring risk perceptions, expected benefits, and perceived-risk attitudes in German-speaking populations. *Polish Psychological Bulletin, 35*, pp. 153-172.

Kraus, L., Fiebig, T., Miruchna, V., Möller, S., & Shabtai, A. (2015). Analyzing End-Users' Knowledge and Feelings Surrounding Smartphone Security and Privacy. *Proceedings of the Workshop on Mobile Security Technologies (MoST).*

Kraus, L., Hirsch, T., Wechsung, I., Poikela, M., & Möller, S. (2014 a). Poster: Towards an Instrument to Measure Everyday Privacy and Security Knowledge. *Symposium On Usable Privacy and Security (SOUPS).*

Kraus, L., Wechsung, I., & Möller, S. (2014 b). A Comparison of Privacy and Security Knowledge and Privacy Concern as Influencing Factors for Mobile Protection Behavior. *Workshop on Privacy Personas and Segmentation, Symposium On Usable Privacy and Security (SOUPS).*

Kraus, L., Wechsung, I., & Möller, S. (2014 c). Using Statistical Information to Communicate Android Permission Risks to Users. *Proceedings of the 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (pp. 48-55). IEEE.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15(4)*, 336-355.

Marshall, C., & Rossman, G. B. (2010). *Designing qualitative research.* Sage publications.

Möller, S. (2005). *Quality of telephone-based spoken dialogue systems.* Springer Science & Business Media.

Möller, S. (2010). *Quality engineering: Qualität kommunikationstechnischer Systeme.* Berlin Heidelberg: Springer.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security (34)*, 47-66.

Mylonas, A., Theoharidou, M., & Gritzalis, D. (2013). Assessing privacy risks in Android: A user-centric approach. *Proceedings of the 1st international workshop on risk assessment and risk-driven testing (RISK),* (pp. 21-37). Springer International Publishing.

Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. . *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 249-256). ACM.

Park, Y. J. (2011). Digital literacy and privacy behavior online. . *Communication Research*.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71(12)*, 1133-1143.

Reiss, S. (2004). Multifaceted nature of intrinsic motivation: The theory of 16 basic desires. *Review of General Psychology, 8, 3: 179.*

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist, 55(1)*, 68.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., & Dolev, S. (2009). *Google android: A state-of-the-art review of security mechanisms.* arXiv preprint arXiv:0912.5101.

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. . *Journal of personality and social psychology, 80(2)*, 325.

Sieger, H. (2015). Perceived security and usage of a mobile payment application. Doctoral dissertation, TU Berlin.

Sieger, H., Kirschnick, N., & Möller, S. (2012). Poster: User perception of usability and security of a mobile payment system. *Symposium on Usable Privacy and Security.*

Sonnleitner, A., Pawlowski, M., Kässer, T., & Peissner, M. (2013). Experimentally Manipulating Positive User Experience Based on the Fulfilment of User Needs. *Human-Computer Interaction–INTERACT*, (pp. 555-562).

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 11). ACM.

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. . *Usenix Security .*

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43(3)*, 389-418.

7. Appendix

Dashboard to aid software architects and programmers during the design of usable and secure applications

The results of the project were used to develop a prototype of a "Usability and UX Dashboard".

Often during the design of usable security and privacy solutions (this is considered as trustworthy ICT in this deliverable) there are several studies conducted to test a trustworthy ICT component regarding usability and/or user experience. In each study different aspects might be considered and usability might be improved iteratively. In contrast to other products, in the field of security and privacy the challenge is, however, that also the threat model has to be taken into account when the product is designed (cf. also Garfinkel & Lipfort, 2014). A security solution might be secure related to a certain threat, but it might not address other threats. Also, in many cases security vulnerabilities are discovered after the solution has been already put into the field.

Thus, it is a complex task to design security systems and designing usable security systems is even more complex - if not impossible without making trade-offs. It is hard for designers and developers to keep track of conducted user studies, their results, their implications, and the threat model.

The Usability and UX Dashboard provides a simple mean to link usability and user experience studies and the documents associated with them (e.g. preparation files, data sheets, analysis outcomes, graphs, etc.). Moreover, is possible to create a threat model in form of a threat tree within the dashboard, from both a security-centered perspective and a user-centered perspective. Thereby, the security-centered perspective is related to a threat analysis from a security engineer's point of view and the user-centered perspective is related to the threats which the users subjectively perceive in the given context, independently of the actual risks. The Usability and UX Dashboard enables software architects and programmers in keeping track of usability and user experience evaluation outcomes for different use cases or sprints and to relate them back to the threat model. By interlinking this knowledge, new ideas can be generated and innovations related to usable and trustworthy ICT are stimulated.

In the following a step-by-step overview of the Usability and UX Dashboard functionalities is provided. It is planned to make the dashboard software available for download on the GTAC website.

As soon as the dashboard is started a dialog appears in which the dashboard user can either select to create a new project, to open an existing project or to exit the program (Figure 25).

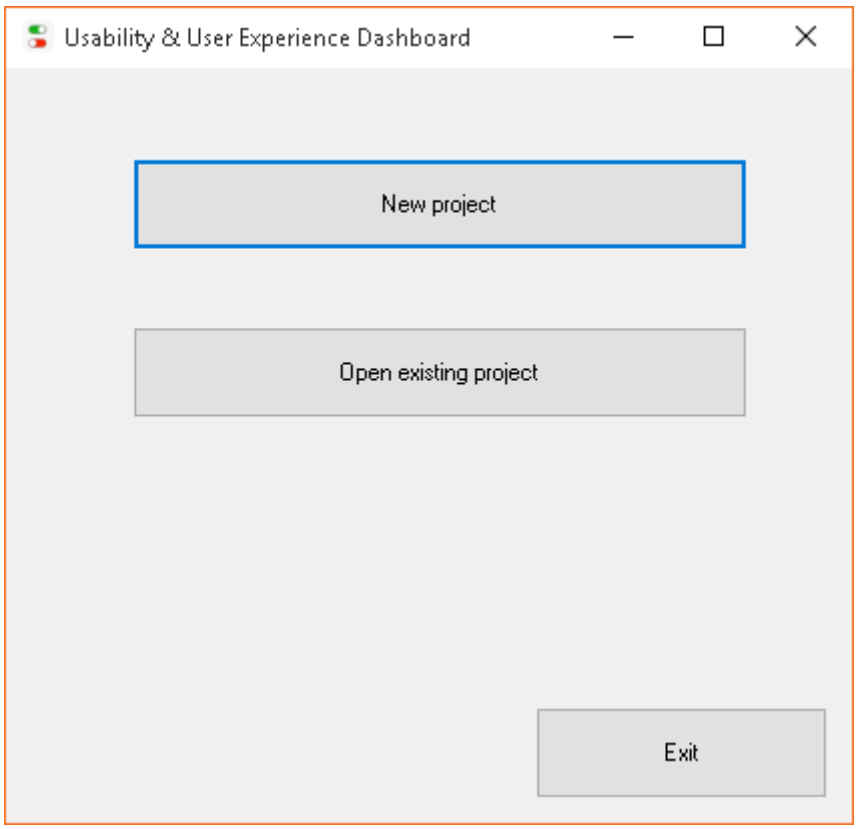

Figure 25 Starting dialog of the Usability and UX Dashboard

When a new project is created, the dashboard user can select which component to include in the project. As the dashboard was designed to support experiments with the GTAC components, the user can either select one of the GTAC components or add a custom component from a drop-down list with visual cues. When the component is selected a name and a description needs to be added.

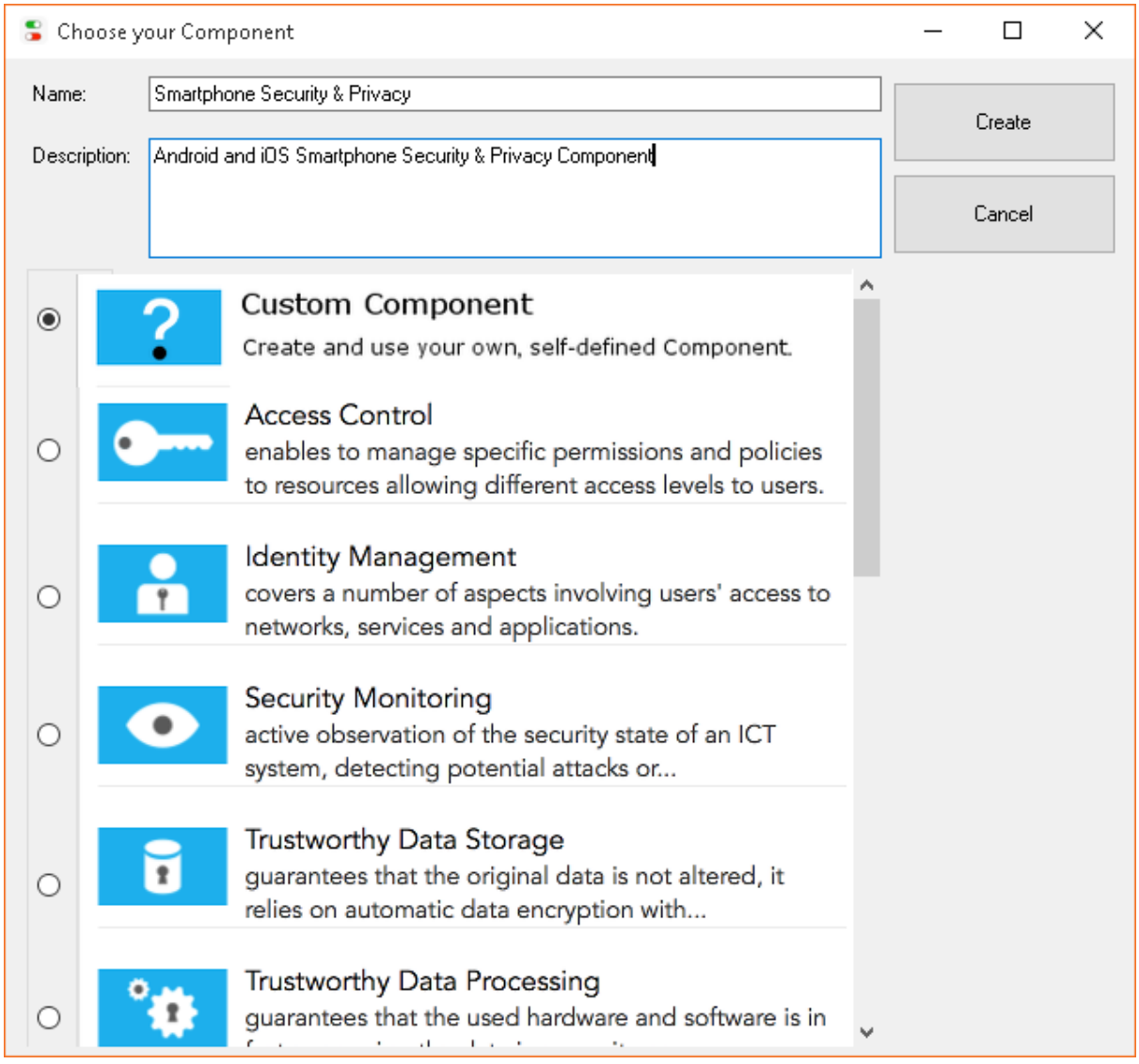

Figure 26 Component selection (either custom component or GTAC component)

As soon as the project has been created with its first component, the dashboard appears on the screen (Figure 27). On the upper left, information about the component under test is provided (Figure 28).

Figure 27 Dashboard view after a new project has been created.

Figure 28 Component information within the dashboard

The dashboard user needs to create different use cases or sprints, before the dashboard can be used. By clicking on the plus in the Use Cases/ Sprint sub-window (Figure 29) a new use case or sprint can be created.

Figure 29 Use case/ sprints sub-window within the dashboard

As soon as this plus button is pressed, a dialog box opens and the dashboard user can define the name of the use case or sprint and add a description (Figure 30).

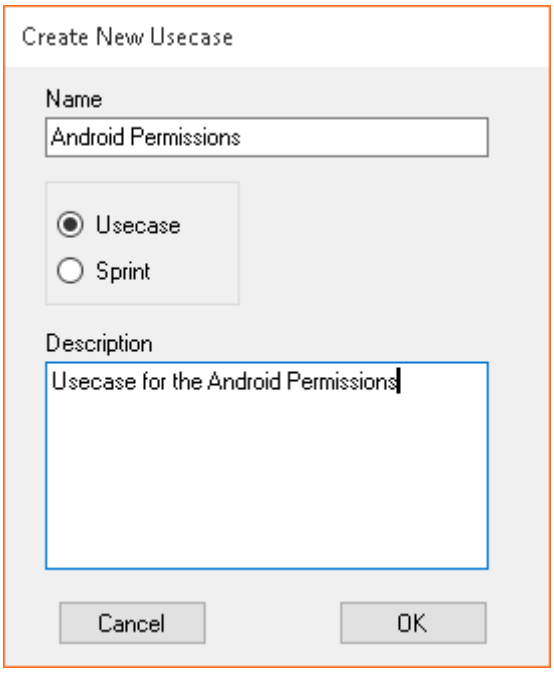

Figure 30 Create new use case or sprint

With each use case or sprint, a usability lifecycle sub-window, an experience model and a threat model is associated.

In the middle of the window, on the upper side, the usability engineering lifecycle (cf. Möller, 2010) is depicted (Figure 31).

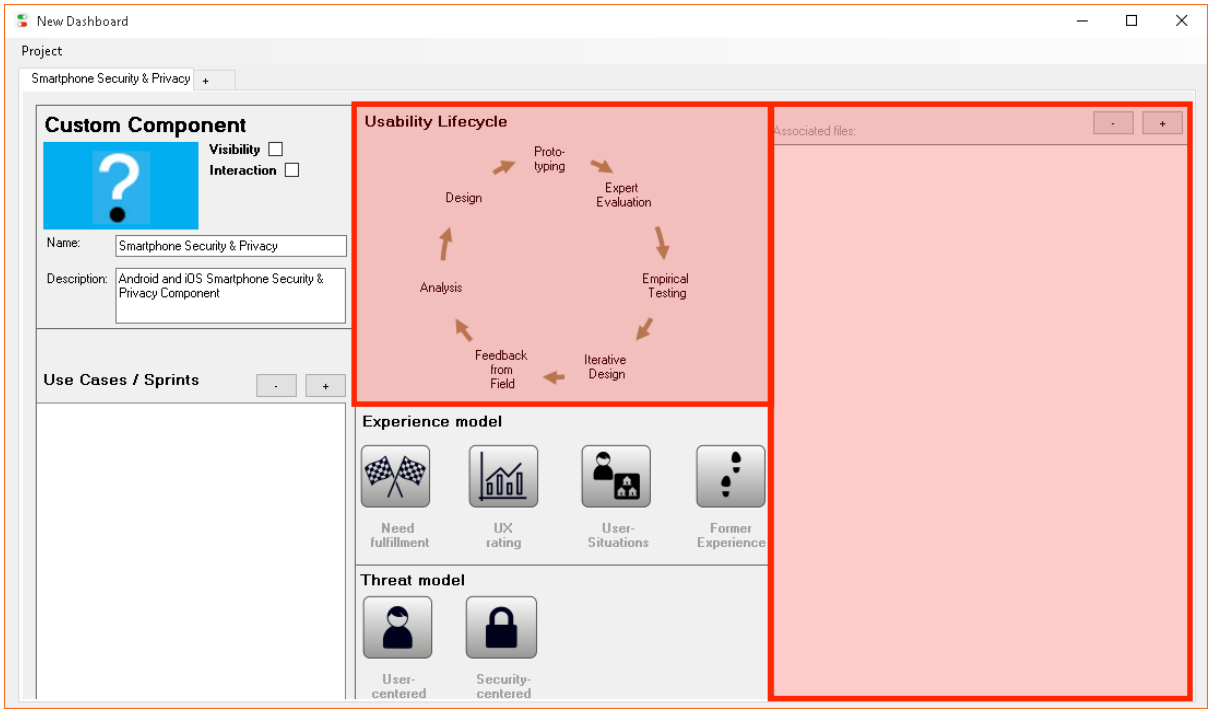

Figure 31 Usability engineering lifecycle on the dashboard

Below the usability engineering lifecycle, the experience model is depicted (Figure 32). Please note that the elements of the experience model refer to the factors that were investigated within ATTPS. Other dashboard users might want to put the focus of their experience model on different factors. Therefore, the dashboard in its current shape should be rather seen as an example of how a dashboard in this context could look like.

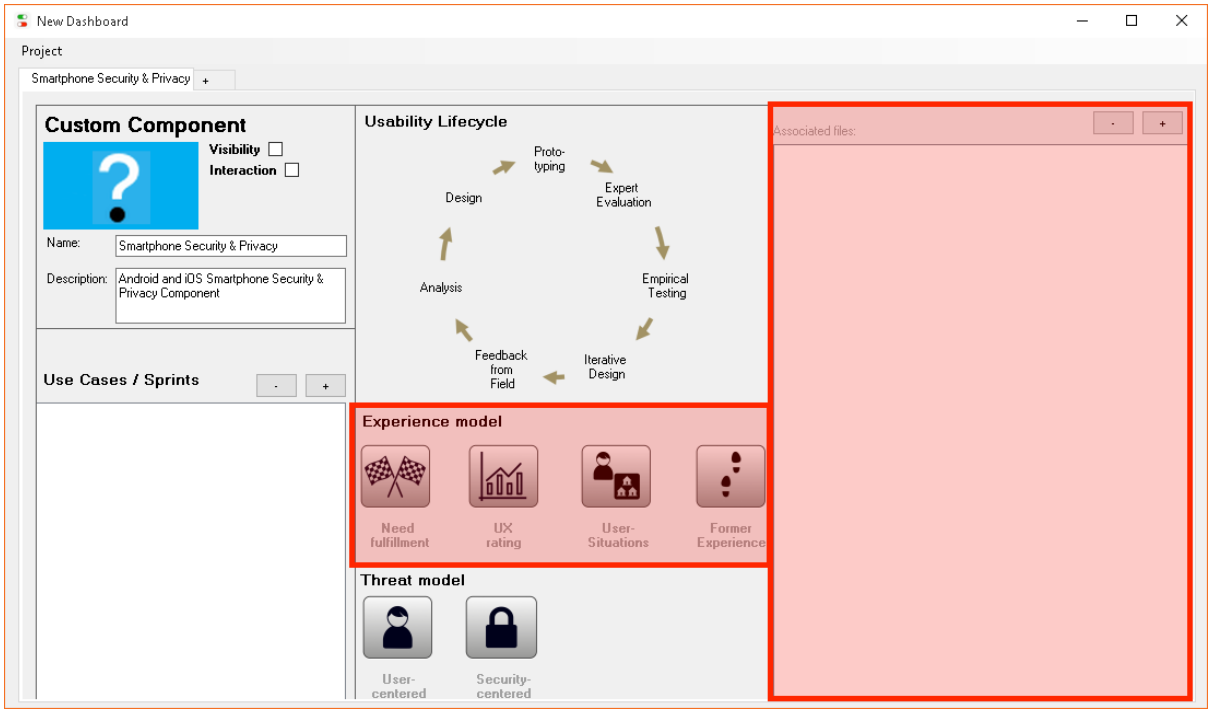

Figure 32 Experience model within the dashboard.

On the bottom in the middle of the dashboard, the threat model is depicted (Figure 33)

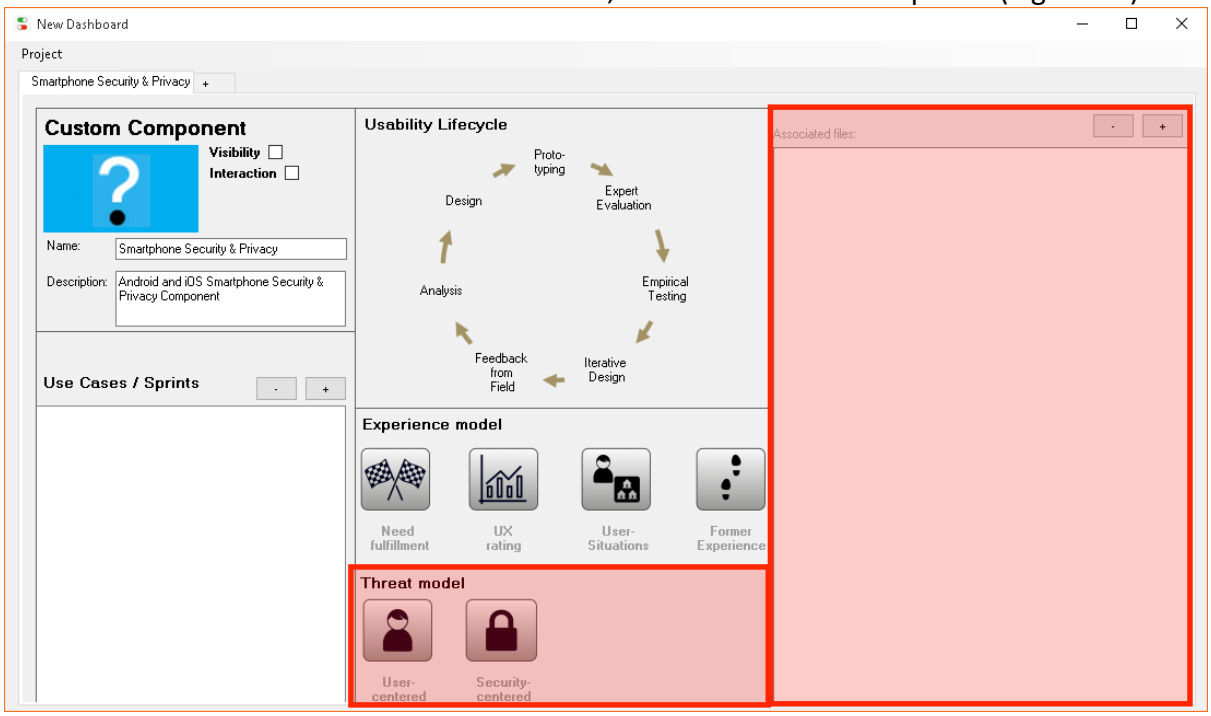

Figure 33 Threat model within the dashboard

As soon as the dashboard user clicks on one of the buttons or factors in the models (cf. Figure 34, Figure 35, Figure 36), the associated files appear in the right sub-window. The files can then be opened by a double click.

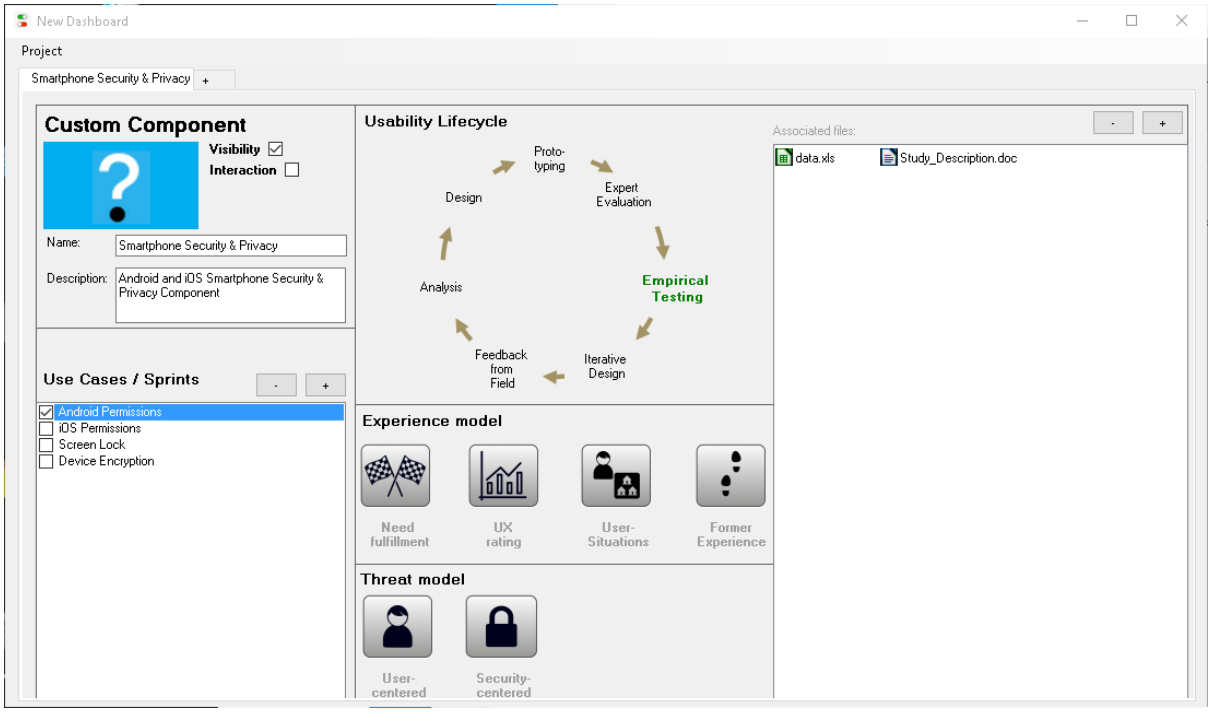

Figure 34 Usability Lifecycle within the dashboard after the user has clicked on "empirical testing"

Figure 35 Experience model within the dashboard after the user has clicked on "Need fulfillment"

For the threat model (Figure 36), the sub-window on the right is divided in two parts. Within the upper part, the associated files are accessible. Within the lower part, the threat tree is shown.

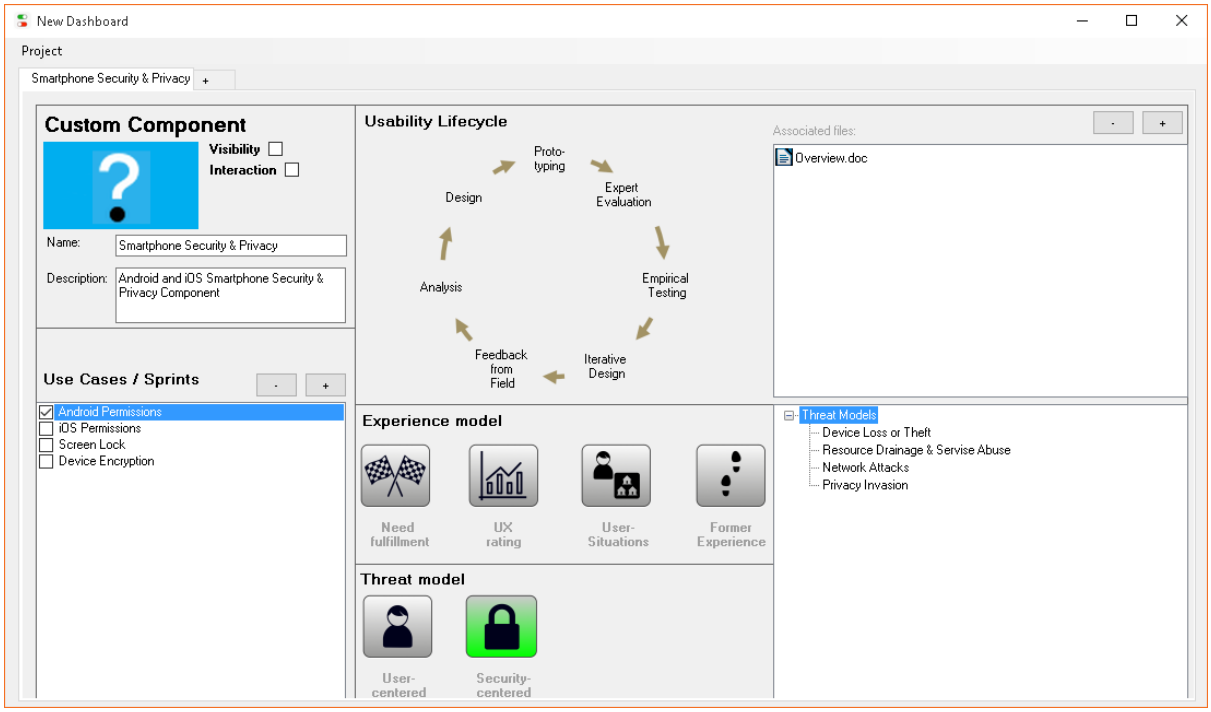

Figure 36 Threat model within the dashboard after the user has clicked on "Security-centered"

Google Scholar search on privacy concern

Conducted at October 1, 2016

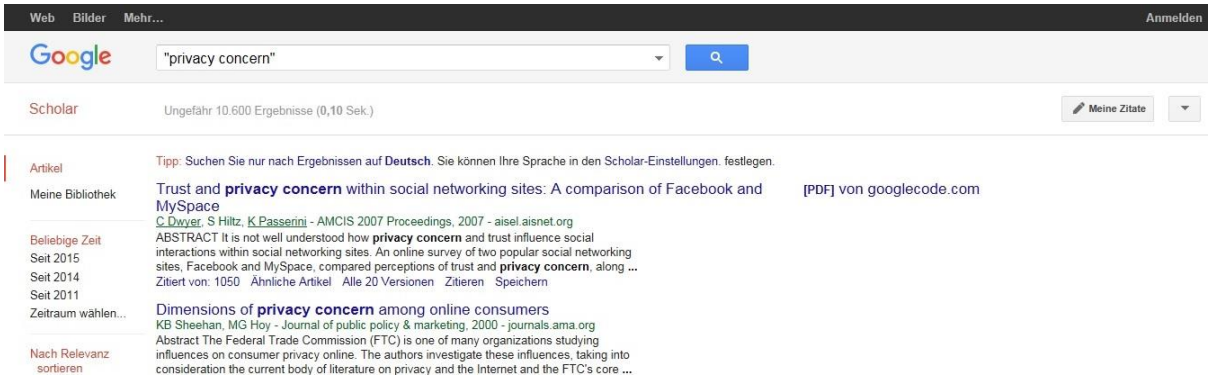

Figure 37 Results for a search on "privacy concern" including the year 2015

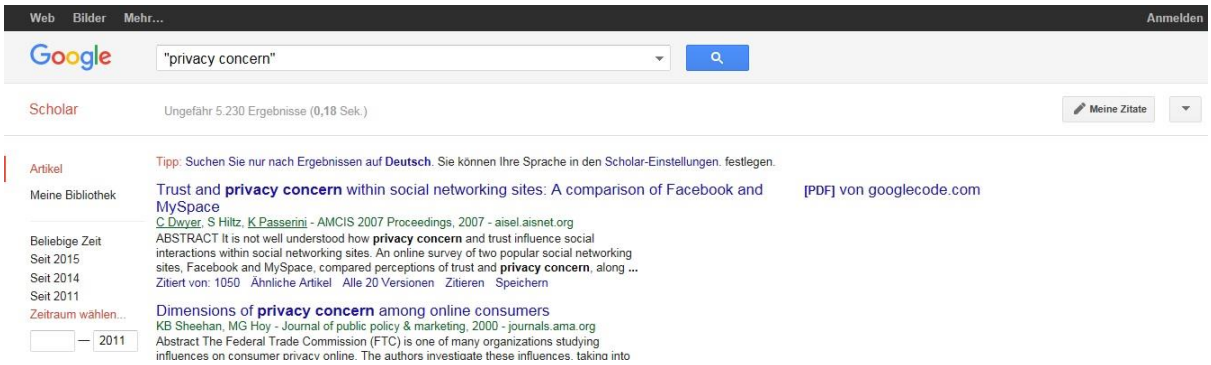

Figure 38 Results for a search on "privacy concern" including the year 2011