User Acceptance Factors for Anonymous Credentials: An Empirical Investigation

Zinaida Benenson, Anna Girard
Friedrich-Alexander-University Erlangen-Nuremberg, Germany
zinaida.benenson@cs.fau.de, anna_girard@hotmail.de

Ioannis Krontiris
Huawei Technologies Düsseldorf GmbH, Munich, Germany
ioannis.krontiris@huawei.com

Abstract

We describe theoretical development of a user acceptance model for anonymous credentials and its evaluation in a real-world trial. Although anonymous credentials and other advanced privacy-enhanced technologies (PETs) reached technical maturity, they are not widely adopted so far, such that understanding user adoption factors is one of the most important goals on the way to better privacy management with the help of PETs. Our model integrates the Technology Acceptance Model (TAM) with the considerations that are specific for security- and privacy-enhancing technologies, in particular, with their "secondary goal" property that means that these technologies are expected to work in the background, facilitating the execution of users' primary, functional goals. We introduce five new constructs into the TAM: Perceived Usefulness for the Primary Task (PU1), Perceived Usefulness for the Secondary Task (PU2), Situation Awareness, Perceived Anonymity and Understanding of the PET. We conduct an evaluation of our model in the concrete scenario of a university course evaluation. Although the sample size (30 participants) is prohibitively small for deeper statistical analysis such as multiple regressions or structural equation modeling, we are still able to derive useful conclusions from the correlation analysis of the constructs in our model. Especially, PU1 is the most important factor of user adoption, outweighing the usability and the usefulness of the deployed PET (PU2). Moreover, correct Understanding of the underlying PET seems to play a much less important role than a user interface of the system that clearly conveys to the user which data are transmitted when and to which party (Situation Awareness).

1 Introduction

In order to build trust in the online environment and to facilitate economic development, it is important to show to citizens that going online is not just convenient, but also trustworthy, and that their data will not be mismanaged or misused, sold or stolen. One

way to achieve this is by incorporating privacy protection mechanisms from the earliest stage of product development, by using Privacy-Enhancing Technologies (PETs) [42].

During the last years, there has been a growing amount of research in the field of PETs enabled by major advances in cryptographic research. PETs provide advanced privacy features such as anonymous protection for real-time communication, privacy-respecting identity management and methods for anonymously retrieving online content.

Yet, PETs are not widely adopted in practice so far. One cannot expect a simple explanation to this, as online privacy is a complex and interdisciplinary issue. Several of the technical aspects have been addressed at a satisfactory degree, but there are still several socioeconomical aspects of PETs adoption that need attention.

In this article we discuss in particular the acceptance factors and the cost-benefit trade-offs involved in adopting such technologies, as perceived by users. Such considerations are technology-specific as well as dependent on the applications in which PETs are deployed [21]. Therefore, in this paper we narrow down the discussion by focusing on a specific PET and on a particular application scenario. More specifically, during the last four years, the EU-funded research project ABC4Trust[1] concentrated on the advancement of anonymous credentials and their applicability in real-world scenarios. In this work we report the first to our knowledge attempt to evaluate the factors affecting user acceptance of anonymous credentials from within a real-world trial that was conducted during the project.

The trial was conducted at the university of Patras during 2013-2014 (in two rounds) where anonymous credentials, also called privacy-respecting attribute-based credentials *Privacy-ABCs* were integrated in the online course evaluation system used by the university to allow students to evaluate their course at the end of the semester without revealing their identity.

The contributions of this work are as follows:

- We develop a rigorous theoretical and methodical framework for evaluation of user acceptance in real-world trials that involve advanced PETs.
- We present the results of the user acceptance evaluation and the related cost-benefit analysis of the anonymous credentials, paying special attention to the relative importance of individual factors.
- From the evaluation results, we draw recommendations for organizations and policy makers concerning integration of advanced PETs into services.

This paper is organized as follows. We first present the Patras trial in Section 2 and consider related work in Section 3. Theoretical development of the user acceptance model is presented in Section 4. Research method is presented in Section 5, and the results on the user acceptance factors are discussed in Section 6. We consider prossible economic trade-offs related to our model of user acceptance in Section 7, discuss the limitations and the implications of our research in Section 8 and conclude in Section 9.

[1] `https://abc4trust.eu/`

2 Privacy-ABCs in the Patras Pilot

Privacy-ABCs are examples of privacy-respecting credential systems that provide untraceability and minimal disclosure. Some specific implementations of Privacy-ABCs are Idemix [11, 12] and U-Prove [9, 32]. Over the last few years, these two systems have been developed to offer an extended set of features, even though these features are named differently and they are realized based on different cryptographic mechanisms.

In 2010, the EU research project ABC4Trust was initiated with the goal to alleviate these differences and unify the abstract concepts and features of such mechanisms. One of the main achievements of ABC4Trust project was to test Privacy-ABCs in real-world situations within the scope of two large-scale user trials and extract valuable experiences regarding the interaction of users and system designers with the technology. One of the user trials was conducted at Patras university in Greece for providing a privacy-respecting course evaluation system.

Course evaluation at universities is still often conducted on paper, but computer-based systems are also becoming a popular alternative. Still, these computer-based systems rarely address user privacy by design, they are mostly based on the trust students have to place on the fairness and policies of the entity that is operating the system. The Patras pilot has employed Privacy-ABCs to design a course evaluation system that offers the technical guarantees that users remain anonymous throughout the process and no identifying information ever reaches the provider of the service. The goal of the pilot was to demonstrate the technology in practice and improve it based on the experiences and feedback received.

The Privacy-ABC technology allowed to implement a course evaluation system (called *CES* in the following) with unique (to the best of our knowledge) properties that insured fairness for both sides, the students and the lecturers. More specifically, Privacy-ABCs allow students to remain anonymous throughout the whole process of course evaluation, at the same time they make sure that only those students that satisfy the policy of the university course evaluation can access the CES. In our case the Patras University had defined the policy that students need to satisfy the following properties: (1) they have registered to the course which they want to evaluate and (2) they have attended at least half of the lectures of that course.

So, on the one side, students get all the necessary guarantees that their anonymity is protected and they can express their opinion freely and on the other side, the lecturers can receive credible evaluation results for their courses, given that only students having attended a meaningful percentage of the class can evaluate it.

The implementation of the Patras pilot required that students collected Privacy-ABCs and stored them in smartcards that they had been provided with. Specifically, through a browser interface (see Figure 1(a)) they collected two credentials issued by the university at the beginning of the semester, one for being enrolled as students at the institution and one for being registered for the specific course. During the semester, they also obtained one attendance unit (implemented as increasing a counter value) per time they attended the class, by waving their smartcard in front of a contactless reader

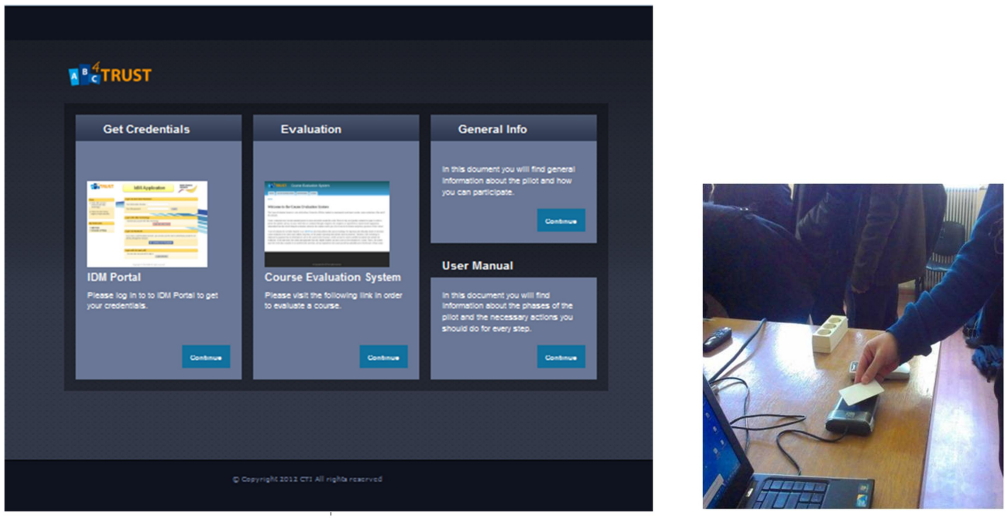

Figure 1: The ABC4Trust Patras Pilot. (a) Browser interface through which students can get their credentials and access the course evaluation system. (b) Students collect attendance units at the beginning of each class.

before entering the lecture room (see Figure 1(b)).

The students were provided also with smartcard readers and they had to install a web-browser plugin. This allowed them to make periodic local backups of their smartcards during the semester, so that in case of loss they can restore their credentials content to a new smartcard. At the end of the semester, the students could use their smartcards to login anonymously onto the service provider, i.e. the CES, and fill the evaluation form. More specifically, during the authentication process over the browser, the students were confronted with a user interface, where they were first presented with the Policy of the CES. Then they could select different attributes from their credentials and authenticate to the CES, revealing only the minimum required information. Overall, in the scenario of the Patras pilot, Privacy-ABCs guarantee the following properties in the protection of students' privacy:

- Pseudonymity: Students don't reveal their identity to the CES, but they present themselves under a random pseudonym. No one else (including a malicious credential issuer) can present a matching pseudonym to hijack the user's identity.
- Selective Disclosure: Students disclose only the minimum required information that is necessary to gain access to the system. In particular, they verify their enrollment and sufficient attendance to the course, without disclosing other information.
- Untraceability: The university, as the issuer of the credentials, is not able to see when and where the students use them. In general, Privacy-ABCs are by default

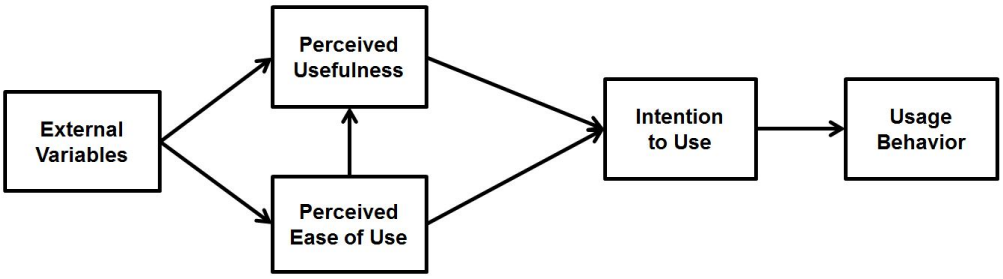

Figure 2: The general framework of the Technology Acceptance Model.

untraceable and service providers cannot track and trace at which sites the user is authenticating.

- Unlinkability: Students can evaluate multiple courses producing a different random pseudonym each time. The CES cannot link the evaluations of two different courses back to the same student.
- Consumption Control: Students can evaluate each course only once. If they conduct a second evaluation, the new evaluation replaces the old one. This means that the students are not able to create multiple pseudonyms based on a single credential. Privacy-ABCs can satisfy this requirement by making sure that for a so-called scope string (e.g., a URL) a student can only register a single pseudonym.
- Prevention of Identity Theft and Credential Pooling: Stealing the credentials from the students is difficult, and the students cannot also easily share their credentials. This is because credentials are bound to a secret key stored in a protected area in the smartcard and one cannot use them without the smartcard. Even if the smartcard is lost or stolen, one needs a secret PIN to access its memory.

3 Related Work

3.1 Acceptance of Information Technologies, Trust and Perceived Risk

User acceptance of information technologies is a very mature research field that has been especially influenced by the Technology Acceptance Model (TAM) [16]. TAM considers *Perceived Ease of Use* and *Perceived Usefulness* of a technology as main factors in user adoption [14]. These two factors positively influence *Intention to Use* the technology, which in turn positively influences the actual *Usage Behavior*. The original TAM [14, 15] also considered *Attitude Towards Using* the technology as a factor affecting Intention to Use. However, this factor was excluded from the model later [46, 45]. Additionally, Perceived Ease of Use indirectly influences Intention to Use through its influence on Perceived Usefulness. The overall TAM framework is depicted in Fig. 2.

The TAM factors are defined as follows:

- *Perceived Ease of Use (PEoU)* is "the degree to which a person believes that using a particular system would be free of effort" [14, p. 320].
- *Perceived Usefulness (PU)* is "the degree to which a person believes that using a particular system would enhance his or her job performance" [14, p. 320]. Depending on the system being evaluated, performance of tasks corresponding to the particular context is considered instead of job performance.
- *Intention to Use*, also called Behavioral Intention in the literature, refers to the "degree to which a person has formulated conscious plans" to use or not to use a specific technology [49, p. 214].
- *Usage Behavior* is the actually observed and measured usage, for example frequency and duration of the usage.

TAM research also considered external variables that may influence Perceived Usefulness and Perceived Ease of Use [46, 45], such as characteristics of the system (e.g., relevance of the system for the task, perceived quality of system's results), individual differences between the users (e.g., age, gender, experience, computer proficiency) or characteristics of the user's environment (e.g., technical and managerial support, influence of other users). Quite often, the actual usage of the system is not considered in the literature, usually because the objective usage data is not available, such that instead of relying on the self-reported system usage, the research concentrates on the Intention to Use, which is considered to be a reliable predictor of the actual system usage.

A more recent technology acceptance model is the Unified Theory of Acceptance and Use of Technology (UTAUT) [47]. UTAUT evolved from the theoretical and empirical investigation of eight technology acceptance models (including TAM) in the organizational setting, and has recently been extended to the consumer context [48].

Although UTAUT is more successful than TAM in terms of the explained variance in usage intention, we use the TAM framework for our study, because we consider two additional acceptance factors, Trust and Perceived Risk, to be especially important for the adoption of security- and privacy-enhancing technologies. Whereas examinations of Trust and Perceived Risk within the TAM framework have a long-standing tradition, integration of these factors into UTAUT is still an emerging research field [30].

Security- and privacy-sensitive scenarios usually involve perceived risk and trust as factors of user participation. User's assets (such as data, money or reputation) can be put at risk, and the decision to participate in such a scenario involves risk assessment and depends on the trust of the participant in other participating parties and in the underlying technology [36, 31]. We consider *Trust* into technology in our study that is defined as a belief that this technology "has the attributes necessary to perform as expected in a given situation in which negative consequences are possible" [31, p. 7]. *Perceived Risk* is defined as "subjective belief of suffering a loss in pursuit of a desired outcome" [36, p. 77].

Although trust and perceived risk have been considered in the context of TAM for more than a decade, their relationship to each other and to the TAM variables is con-

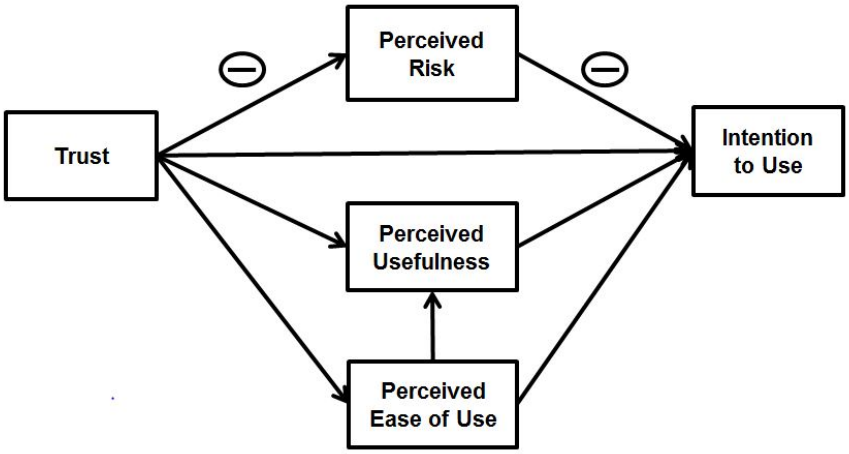

Figure 3: Integration of Trust and Perceived Risk into the Technology Acceptance Model [36]. Negative influence is labeled as (-), non-labeled arrows depict positive influence.

tradictory in different research models, such that sometimes, for example, risk is said to influence trust [17] or vice versa [36].

A recent meta-analysis of the trust-risk relationship clarifies this issue [33]. According to the meta-analysis, the research model by Pavlou [36] that integrates Trust and Perceived Risk into the TAM in the context of online shopping (see Fig. 3), outperforms all other relationship variants. In Pavlou's model, that we use in our study, Perceived Risk (PR) decreases Intention to Use, whereas Trust increases PU and PEoU, reduces PR and also has a direct influence on the Intention to Use.

3.2 Acceptance of PETs and Security Technologies

User acceptance of privacy-enhancing technologies has rarely been considered in the literature so far. Most relevant for this study are the investigation of RFID PET acceptance by Spiekermann [41] and a recent qualitative study by Harbach et al. [24] on the adoption of the German national identity cards.

Spiekermann [41] considers user acceptance of advanced RFID PETs in the hypothetical scenario of RFID-based retail. In an experimental between-group setting, users are presented with a documentary about the RFID technology, its after-sales benefits and two different PETs (one per group) that can be used for controlling the information flow from the RFID tags once the products to which they are attached are purchased by the customer. Main research question concerns the influence of the *Perceived Control* through different PETs over the read-out of the RFID tags on consumers' intention to adopt the after-sales RFID services. We will return to the notion of Perceived Control in Section 4.

Independently and concurrently to our work, Harbach et al. [24] conducted focus

groups and interviews with German citizens and service providers concerning the adoption of the privacy-preserving authentication services integrated in the new German national identity cards. Although these services are technically less advanced than Privacy-ABCs [38], it is possible to integrate Privacy-ABCs into the eID infrastructure [7]. Harbach et al. report several barriers to the user adoption of the privacy-preserving eID authentication services. We discuss their findings in more detail in Section 8.

As Privacy-ABCs provide authentication services, another stream of related work is user acceptance of authentication mechanisms and other security mechanisms. Thus, Lee and Kozar [26, 27] consider user adoption of anti-spyware using the Theory of Planned Behavior and the Innovation Diffusion Theory as theoretical background. Although their research model does not build on the TAM, they find, for example, that Perceived Ease of Use is not an important factor in user adoption, whereas other factors such as the visibility of the anti-spyware adoption by other people and the belief into own ability to use the anti-spyware play an important role.

Herath et al. [25] develop and verify a user acceptance model for an email authentication service. This external service helps the users to verify the legitimacy of an email. They combine TAM with the Technology Threat Avoidance Theory and show, for example, that the email risk perception, combined with the high PU and PEoU of the service, play an important role in the user acceptance.

Most relevant for our study is the investigation of the acceptance of single sign-on by Sun et al. [44]. They conducted a laboratory experiment and a qualitative study that resulted in a tentative user acceptance model for single sign-on. We consider this model when developing our research model in Section 4.

Finally, our own previous work should be mentioned here. The results of the first run of the Patras trial are reported in [5]. There, we developed (and subsequently partially rejected) our first user acceptance model. We also validated and subsequently improved measurement scales for some constructs, such as PU, PEoU, Trust and Understanding of Privacy-ABCs (see also Section 5). Furthemore, a technical report on the second round of the Patras trial can be found in [43]. This report concentrates more on the usability evaluation of the Privacy-ABC system and presents a simplified user acceptance model with the corresponding discussion.

3.3 Economic Analysis of PETs

Economic considerations of privacy trade-offs for consumers and service providers are presented in [2, 21]. Especially, both data protection and data sharing incur costs and benefits on both sides, depending on the concrete technology and concrete applications. Furthermore, advanced PETs such as Privacy-ABCs are considered as a means that can simultaneously decrease the costs from data sharing for the consumers, still allowing the businesses to process consumer data and even to profile customers, as long as the customers remain pseudonymous and their online pseudonyms cannot be linked to their real offline identities.

Acquisti [1] proposes a framework for rational consideration of privacy trade-offs that can also be considered from the viewpoint of user acceptance of privacy-enhancing

technologies. Here, the utility u_t of completing a transaction t using some (privacy-enhancing or not) technology d is represented as follows:

$$u_t = \delta[v_E(t), p^d(t)] + \gamma[v_E(a), p^d(a)] - c_t^d \quad (1)$$

In the above equation, $v_E(t)$ represents the expected payoff (or value) of completing the transaction, $p^d(t)$ is the probability of completing t using technology d, $v_E(a)$ is the payoff of retaining privacy (or anonymity) for this transaction, $p^d(a)$ is the probability of successfully protecting privacy with technology d, and c_t^d are the costs of using the technology d. The unspecified functional forms δ and γ take into account additional unknown factors that influence the relation between the expected payoffs and the corresponding probabilities.

As noted by Acquisti et al. [3], the payoffs and probabilities in the above equation can also be considered as subjective values as perceived by the user. This viewpoint allows to make a connection to the variables of the extended TAM from our study. We discuss this possibility in more detail in Section 7.

3.4 Usability Evaluation and Understanding of Anonymous Credentials

Petterson et al. [37] and Graf et al. [23] investigate in the scope of the EU projects PRIME and PrimeLife, respectively, challenges in designing usable interfaces and user interaction for PETs. Understanding PET-related terms and the complex background mechanisms are identified as factors influencing the interaction of the users with the technology. Wästlund et al. [52, 51] study the users' mental models of the data minimization property of Privacy-ABCs and show that the right mental models are difficult to convey, but the carefully designed user interfaces can help here. The ABC4Trust project builds on the results of PRIME and PrimeLife. However, the detailed presentation of usability properties of the Privacy-ABC system is out of scope of this paper and is considered in Stamatiou et al. [43].

4 Theoretical Background

4.1 Adapting the TAM to the PETs

As presented in Section 3.1, TAM considers *Perceived Ease of Use* and *Perceived Usefulness* of a technology as main factors in user intention to use the technology. Whereas the concept of Perceived Ease of Use is independent of the considered technology, Perceived Usefulness needs a special consideration in the context of security- and privacy-enhancing technologies.

Although the TAM has been widely used for investigation of different technologies, and some of its elements were considered as acceptance factors for privacy-enhancing technologies (Section 3.2), there is no explicit extension of the TAM to the adaption of

these technologies. Security- and privacy-enhancing technologies have a unique characteristic that has not been considered in the TAM context yet: They rarely serve *primary* user goals. The primary goal of the user may be communicating with peers or colleagues via email or social networks, exchanging files, making purchases or managing a banking account, whereas security- and privacy-enhancing tools such as authentication services, anti-virus software or anonymizers work in the background, protecting the users and thus facilitating the successful execution of the primary goal. Thus, the definition of Perceived Usefulness as presented previously is ambiguous: "the degree to which the usage of a particular system would enhance the task performance" refers to the primary task, whereas security or privacy measures that the user has to apply serve the secondary task, which is the system and the user protection.

In the Patras pilot, the primary goal of the participants for the usage of Privacy-ABCs was course evaluation, and the secondary goal was privacy protection during the course evaluation. Therefore, we define two types of Perceived Usefulness as factors of user acceptance:

- *Perceived Usefulness for the Primary Task (PU1)* is the degree to which a person believes the system to be useful for the primary task (in the Patras trial, for course evaluation).
- *Perceived Usefulness for the Secondary Task (PU2)* is the degree to which a person believes the system to be useful for the secondary task (in the Patras trial, for privacy protection).

An interesting question is whether the usefulness for privacy protection should be defined with respect to the course evaluation scenario. We decided against this option, because we think that the belief in the ability of a particular technology to protect one's privacy is independent from the particular scenario, as long as this scenario fits the purpose of the technology.

According to the original TAM (Fig. 2 on page 5) we formulate the following hypotheses:

- H1: PU1 is positively related to the Intention to Use Privacy-ABCs for Course Evaluation.
- H2: PU2 is positively related to the Intention to Use Privacy-ABCs for Course Evaluation.
- H3: PEoU is positively related to the Intention to Use Privacy-ABCs for Course Evaluation.
- H4: PEoU is positively related to PU1.

We also hypothesize that PU2 will have an indirect effect on the Intention through a direct effect on PU1, because PU2 is conceptually a facilitator of PU1:

- H5: PU2 is positively related to PU1.

4.2 Trust and Perceived Risk

To investigate the role of trust and risk in the user adoption of Privacy-ABCs, we decided to adapt the framework of Pavlou [36] that integrates Trust and Perceived Risk into the TAM in the context of online shopping, see Fig. 3 on page 7. According to this framework, Trust into the system positively influences all three TAM variables: Perceived Usefulness, Perceived Ease of Use and Intention to Use. In our case we hypothesize that both, PU1 and PU2, will be influenced. The reasoning is that a trustworthy system is more useful for both, primary and secondary tasks, than an untrustworthy one, and it also requires less mental effort from the user, as there is no need to worry about a possible fraud or to look for the signals of an attack. This makes the system easier to use. Moreover, there is a negative relationship between the Trust and the Perceived Risk (PR): the more trustworthy the system is perceived to be, the less risky seems its usage. PR is also considered to have a direct negative influence on Perceived Usefulness and on the Intention to Use. We hypothesize that for our model, the negative influence of Perceived Risk will decrease PU2.

We formulate the following hypotheses accordingly:

- H6: Trust in the Privacy-ABC System is positively related to the Intention to Use Privacy-ABCs for Course Evaluation.
- H7: Trust in the Privacy-ABC System is positively related to PU1.
- H8: Trust in the Privacy-ABC System is positively related to PU2.
- H9: Trust in the Privacy-ABC System is positively related to PEoU.
- H10: Trust in the Privacy-ABC System is negatively related to PR.
- H11: PR is negatively related to Intention to Use Privacy-ABCs for Course Evaluation.
- H12: PR is negatively related to PU2.

4.3 Additional Acceptance Factors

As mentioned in Section 3.2, we use the TAM extension developed by Sun et al. [44] for the single sign-on scenario to extend our research model further. Analyzing the results of a qualitative study on the user adoption of single sign-on, they hypothesized that the Value of Personal Information (i.e., the value of the account into which the user signs in), Perceived Privacy Control (the possibility to limit the data flow to the provider) and Perceived Security Protection have an impact on Perceived Risk. Moreover, they noticed that users' security misconceptions negatively impact their adoption intention. It is important to note, however, that these extensions were not validated by their authors, such that the extensions are tentative. In the following, we consider analogous factors from the Privacy-ABCs scenario and place them into our research model.

Importance of Anonymity in Course Evaluation In the Patras trial, the asset that should be protected during the course evaluation is user's anonymity. Thus, we think that the Value of Personal Information [44] is analogous to the extent to which a person values his or her anonymity protection.

Situation Awareness We note that although the goal of the Privacy-ABC technology is to give the users more control over their personal data, the Patras trial did not give the students a lot of possibilities to exercise this control, apart from the choice to participate or not to participate in the trial. The reason for this is that almost all information that the students revealed about themselves during the pilot was determined in advance. Thus, we do not have the possibility to investigate Perceived Control as a factor of user adoption.

However, Spiekermann [41] describes a sub-category of Perceived Control that fits the Patras trial quite well. *Situation Awareness* is defined as "personal perception to be informed about what is going on" [41, p. 134]. In connection with Privacy-ABCs, Situation Awareness includes knowing which information will be disclosed in order to get a credential, who receives the data, which data is stored on the smart card, etc. Hence, we consider Situation Awareness to be analogous to Perceived Control in the trial scenario.

Perceived Anonymity In the Privacy-ABCs case, Perceived Security Protection identified by Sun et al. [44] turns into Perceived Anonymity, as this is the protection goal of Privacy-ABCs.

Understanding of Privacy-ABCs It is common knowledge that people do not have to understand exactly how a technology works in order to be able to use it. Much more important than the exact understanding is the development of a *mental model* of the technology that enables the user to use it correctly [50]. Mental models are representations of reality in people's minds, their conceptions about how things work. Right mental models of anonymous credentials seem to be especially difficult to convey [51].

Although the exact technical knowledge may not play an important role in user adoption of privacy- and security-enhancing technologies, users' *misunderstanding* of some key concepts may result in poor adoption. For example, Sun et al. [44] discovered that some users think that their login credentials are given to every participating party when they use single sign-on, which lead to (wrongly) perceived additional insecurity. Therefore, we investigate Understanding of Privacy-ABCs as a possible factor of user adoption that directly positively influences Intention to Use.

According to the above considerations, we formulate the following additional hypotheses:

- H13: Importance of Anonymity is positively related to PR.
- H14: Situation Awareness is negatively related to PR.

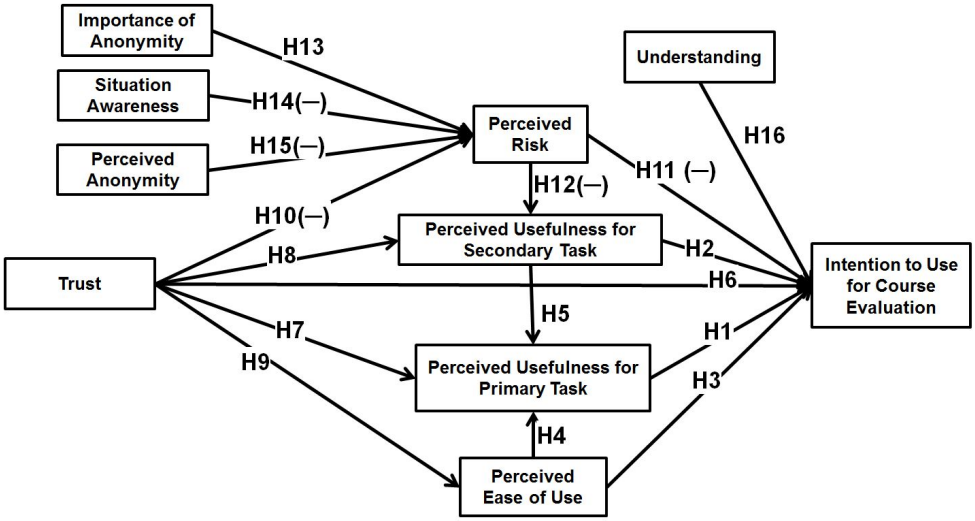

Figure 4: Research model for user acceptance of Privacy-ABCs for course evaluation. Negative relations are labeled with (–).

- H15: Perceived Anonymity is negatively related to PR.
- H16: Understanding of Privacy-ABCs is positively related to Intention to Use.

The resulting research model is presented in Fig. 4.

5 Method

We developed a quantitative standardized questionnaire that the participants of the Patras trial filled in after the end of the pilot. In this section we present the structure of the questionnaire (Section 5.1), measurement scales that we used in the questionnaire (Section 5.2) and the demographic characteristics of the participants (Section 5.3).

5.1 Structure of the Questionnaire

The questionnaire consisted of two main parts: the first part was devoted to the questions about specific Privacy-ABCs usage by the students, and the second part considered general questions not related to the system usage.

More precisely, in the first part the following topics were investigated:

- Usage behavior: was the system used at all, which functions were used (for example, the backup function for the smartcard);
- Understanding of the Privacy-ABC technology: knowledge questions that will be presented in more detail in Section 6.2 on page 20;

- Preference for paper-based or for Privacy-ABCs-based course evaluation;
- Scales presented in Table 1 below;
- Reliability questions (was the system working correctly, were any crashes or other problems encountered);
- Usability questions presented in Table 3 on page 24.

The second part surveyed the usage of Internet services such as online social networks and online banking, Internet privacy concerns (using the scale by Dinev and Hart [18]), privacy-aware benavior on the Internet (including usage of PETs), and, finally, age and gender.

5.2 Measurement Scales

The constructs considered in this research were measured on a 5-point Likert scale ranging from "strongly disagree" to "strongly agree", see also Table 1. Perceived Ease of Use, Perceived Usefulness for Primary Task, Perceived Usefulness for Secondary Task and Intention to Use closely follow the scales by Venkatesh et al. [46, 45], whereas Trust and Perceived Risk are measured using a single item respectively, adapted from Pavlou [36].

The scale for Perceived Anonymity was adapted from the "Sense of Security" construct by Bosmans et al. [8]. Situation Awareness was constructed using different (slightly changed) items from the PET-USES questionnaire [53]. Understanding of Privacy-ABCs is a newly developed knowledge index that is presented in Section 6.2.

We run an exploratory factor analysis with a Varimax rotation to ensure the one-dimensionality and hence the validity of the measured constructs. We also conducted several reliability tests to assure the quality of each measurement scale. All reported multi-item scales fulfill the following quality criteria: one-dimensionality (Kaiser-Meyer-Olkin criterion > 0.5, total variance explained $> 50\%$) and reliability (Cronbach's $\alpha > 0.7$) [20]. For all further analyses, we calculated construct scores as the average value of corresponding items. More information about the quality criteria can be found in Appendix A.

5.3 Sample Characteristics

60 computer science students enrolled in the course "Distributed Systems I" were given an introductory lecture on Privacy-ABCs and 45 of them decided to take part in the trial. They were given smart cards and corresponding readers, as well as supporting material (manual and videos). The printouts of the questionnaire were distributed to the pilot participants at the end of the semester. We received 30 filled out questionnaires. Thus, all further descriptions relate to the sample size of 30 subjects (23 male, 7 female, 23 years old on average).

Apart from the usual demographic questions concerning age and gender, some other characteristics of the trial participants are important in order to consider external validity

Intention to Use (adpated from [46, 45]);
Assuming that the Privacy-ABC system is available for course evaluations, I intend to use it.
I would use the Privacy-ABC system for course evaluations in the next semester if it is available.
Given that the Privacy-ABC system is available for course evaluations, I would use it.
Perceived Usefulness for Primary Task (adapted from [46, 45])
Using Privacy-ABCs improves the performance of course evaluation.
Using Privacy-ABCs enhances the effectiveness of course evaluation.
I find Privacy-ABCs to be useful for course evaluation.
Perceived Usefulness for Secondary Task (adapted from [46, 45])
Using Privacy-ABCs improves my privacy protection.
Using Privacy-ABCs enhances the effectiveness of my privacy protection.
I find Privacy-ABCs to be useful in protecting my privacy.
Perceived Ease of Use (adapted from [46, 45])
Interacting with the Privacy-ABC System does not require a lot of my mental effort.
The Privacy-ABC System is easy to use.
I find it easy to get the Privacy-ABC System to do what I want to do.
Perceived Risk (adapted from [36])
I would see the decision to evaluate the course with the Privacy-ABC System as a risky action.
Trust into the Privacy-ABC technology (adapted from [36])
The Privacy-ABC System is trustworthy.
Perceived Anonymity (adapted from [8])
Privacy-ABCs are able to protect my anonymity in course evaluation.
With Privacy-ABCs I obtain a sense of anonymity in course evaluation.
Privacy-ABCs can prevent threats to my anonymity in course evaluation.
Situation Awareness (adapted from [53])
With Privacy-ABCs, I always know which personal information I am disclosing.
I find it easy to see which information will be disclosed in order to get a credential.
Privacy-ABCs let me know who receives my data.
The Privacy-ABC system gives me a good overview of my personal data stored on my Smart Card.
I can easily find out when (e.g., at which date) I have received a credential via the University Registration System.
I get a good overview of who knows what about my private information from the Privacy-ABC System.
I can easily see which and how many Privacy-ABC credentials I have been issued.

Table 1: Measurement scales for the adapted TAM; all items are measured on a 5-point scale ranging from 1 = "strongly disagree" to 5 = "strongly agree". Mean values and standard deviations for the scales are presented in Table 2 on page 18.

of the study. Important user attributes are for example privacy concerns and privacy-aware behavior in general, and especially usage of privacy-enhancing technologies. We expect the trial participants to exhibit more privacy-aware behavior than an average Internet user. A high level of privacy concerns may influence student's interest in the trial participation.

Most participants are active users of Internet services. Almost all students (28) use online storage services such as Dropbox, 25 participate in online social networks, 23 shop online, and 17 use online banking. They expressed a middle to high level of Internet privacy concerns ($m = 4.03$, $\sigma = 0.86$)[2] on a 5-point Likert scale developed by Dinev and Hart [18].

Only three participants said that they have used a privacy protection tool before the Patras trial. All three of them use TOR, and one additionally mentioned ad-block plug-ins. However, most participants exhibit some other kinds of privacy-aware behavior: 29 out of 30 said that they sometimes delete cookies, 27 sometimes or often clean browser history and 23 sometimes or often use their browser in the private mode. 26 participants said that they sometimes provide fake information when creating a web account.

20 students reported that they participated in paper-based course evaluation before, and seven students already participated in an electronic course evaluation. Most students (21) agreed or strongly agreed that participating in course evaluations is important to them ($m = 3.87$, $\sigma = 0.78$), and 28 participants indicated that protection of anonymity during course evaluations is important (9) or very important (19) for them, with the remaining two participants reporting a neutral attitude ($m = 4.57$, $\sigma = 0.63$).

6 Results on User Acceptance Factors

In this section we explore the relations between the measured constructs and their role in the user acceptance of Privacy-ABCs. We conducted bivariate non-parametric correlations (two-tailed) using Kendall's correlation coefficient (τ), because this test does not require normal data distribution and works for ordinal data and small sample sizes [20]. Despite having directed hypotheses, we decided to conduct two-tailed instead of one-tailed tests in order to account for unexpected results in the other direction [29, 40]. For example, we cannot be sure that the understanding of the Privacy-ABC system will be positively correlated to the intention to use, as better understanding of the system features can actually also lead to a desire to use a system with privacy guarantees that are perceived to be better (e.g., paper-based course evaluation).

Correlation coefficients can also interpreted as effect sizes: $0.1 < \tau \leq 0.3$ indicates a small effect size, $0.3 < \tau \leq 0.5$ a medium and $\tau > 0.5$ a large effect size [13].

Apart from the correlation coefficient τ we report the significance level p of the correlations. The highest significance level is indicated by $p < 0.01$, which means that the probability of the corresponding correlation to occur by chance is less than 1%. We also consider significance level $p < 0.05$. Significance level $p \geq 0.5$ is considered non-significant.

[2] m denotes mean value, σ denotes standard deviation

As we conducted multiple correlation tests with a relatively small sample size, we controlled for alpha error (Type 1 error, or false positive) inflation using Benjamini and Hochbergs False Discovery Rate (FDR) [6]. The FDR is less conservative and has more power than, for instance, the Bonferroni correction, and is especially appropriate for a large number of variables and a high portion of statistically significant results, as in our case [34, 22]. In this procedure all p-values are ranked from the smallest to the largest. In order to adapt for multiple testing, each p-value is multiplied by the total number of tests (here 45) and divided by its rank.

A post hoc power analysis revealed that with the sample size of N=30, an alpha error probability of 0.05, and the significant effects average correlation of 0.460 the study achieved a statistical power of 0.75 [19], which almost meets the desired standard of 0.80 [13]. Thus, we are reasonably confident that our study achieved enough power to detect the most important effects.

Unfortunately, we did not have enough data for a deeper analysis, such as multiple regressions or structural equation modeling, as the sample size of 30 participants is too small.

6.1 Hypotheses Testing

According to the hypotheses from the Section 4, we looked into the correlations between the constructs as depicted in Fig. 4 on page 13. The results are shown Table 2 and in Fig. 5.

We found statistically significant correlations at $p < 0.05$ or at $p < 0.01$ significance level for hypotheses H1, H2, H3, H4, H5, H7, H8, H9, H11, H12, and H15. Hypotheses H6, H10, H13, H14 and H16 are not supported.

We also found a number of other interesting correlations between the constructs. Especially, Perceived Risk is correlated almost to the same constructs to which Trust is correlated. This indicates that Trust and Perceived Risk both play an important role in user acceptance of Privacy-ABCs, but they seem to be more decoupled from each other in the course evaluation situation than in the web shopping situations considered by Pavlou [36]. One possible reason for the absence of the relation between Trust and Perceived Risk (H10 rejected) might be that the participants did not consider course evaluation as a risky situation at all, independently of the technology that is used for this task. The absence of correlation between Trust and Intention to Use (H6 rejected) occurred after the FDR correction was applied, so probably we have a false negative here (this needs further investigation).

Considering the results on Trust and Perceived Risk in more detail as depicted in Fig. 6, we can see that cumulatively, 80% of the participants consider the situation as not risky, and that 80% of the participants trust the system.

The absence of correlation between Importance of Anonymity and Perceived Risk (H13 rejected) can be explained by the fact that 28 out of 30 participants indicated that protection of anonymity during course evaluations is very important (19) or important (9) for them, with the remaining two participants reporting a neutral attitude, making this variable quite homogenous.

	m	σ	IU	PU1	PU2	PEoU	TR	PR	PAn	SAw	Und
IU	4.34	.59	–	–	–	–	–	–	–	–	–
PU1	4.10	.66	.726** (H1)	–	–	–	–	–	–	–	–
PU2	3.93	.74	.420* (H2)	.362* (H5)	–	–	–	–	–	–	–
PEoU	3.80	.69	.498** (H3)	.558** (H4)	.331	–	–	–	–	–	–
Tr	4.13	.73	.326 (H6)	.409* (H7)	.409* (H8)	.609** (H9)	–	–	–	–	–
PR	1.80	.99	-.444* (H11)	-.381* (new)	-.450* (H12)	-.407* (new)	-.308 (H10)	–	–	–	–
PAn	4.20	.46	.206	.191	.455* (new)	.196	.444* (new)	-.383* (H15)	–	–	–
SAw	3.87	.63	.319	.317	.309	.304	.288	-.248 (H14)	.403* (new)	–	–
Und	0.51	.45	-.006 (H16)	.019	.140	-.024	.081	-.134	.346	.175	–
IAn	4.57	.63	.154	.150	.102	.121	.228	-.098 (H13)	.022	.036	-.252
Significance levels: * $p < 0.05$; ** $p < 0.01$ Correlation strength: $0.1 < \tau \leq 0.3$ weak, $0.3 < \tau \leq 0.5$ moderate, $\tau > 0.5$ strong											

Table 2: Correlations between the extended TAM constructs. Notation: m = mean value, σ = standard deviation, IU = Intention to Use, PU1 = Perceived Usefulness for Primary Task, PU2 = Perceived Usefulness for Secondary Task, PEoU = Perceived Ease of Use, PR = Perceived Risk, PAn = Perceived Anonymity, SAw = Situation Awareness, Und = Understanding, IAn = Importance of Anonymity. Additionally to the hypotheses discovered correlations are denoted as "new". Understanding was coded as 0 = incorrect answer (including "don't know"), 1 = correct answer, all other items were rated from 1 = "strongly disagree" to 5 = "strongly agree".

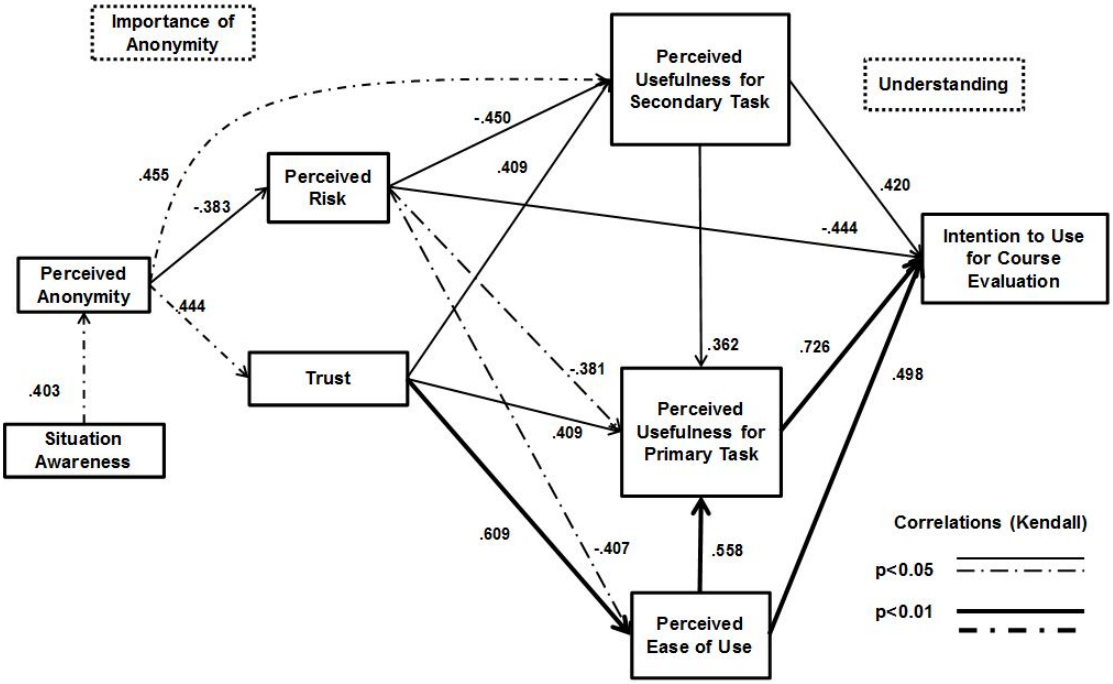

Figure 5: Significant correlations between the constructs of the adapted TAM (Section 4). Additional (not present in the initial model) correlations are depicted with dot and dash lines. Effect sizes (Kendall's τ) are depicted near the corresponding arrows. The arrows do not indicate that we established causal relationships (as this is impossible to do using correlation analysis). Instead, they indicate the theoretical direction of the hypotheses for the cases where existing hypotheses are supported, and the hypothesized direction of the relationships (explained in the text) for additional correlations.

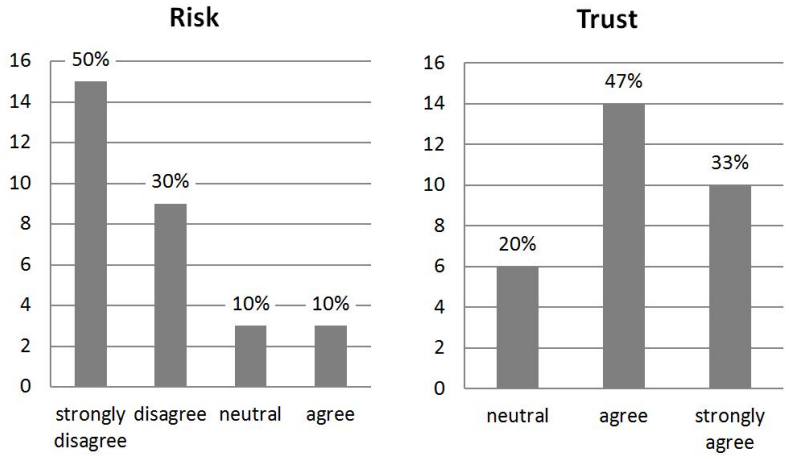

Figure 6: Descriptive data for user perception of the risk connected to the participation in the trial and the trustworthiness of the Privacy-ABC system. Most users disagreed with the statement that course evaluation using Privacy-ABCs is a risky situation, and agreed with the statement that the Privacy-ABC System is trustworthy.

There is also no correlation between Perceived Risk and Situation Awareness (H14 rejected). Instead, Situation Awareness is correlated to Perceived Anonymity, which is in turn correlated to Perceived Risk. Although we do not have any possibility to establish causal relations between the variables, we can hypothesize that higher Situation Awareness leads to higher Perceived Anonymity, as users might feel more anonymous if they have a clear picture of the data flow in the system. According to H15, higher Perceived Anonymity reduces Perceived Risk, such that Perceived Anonymity might mediate the relationship between Situation Awareness and Perceived Risk.

As Perceived Anonymity is significantly correlated to Perceived Risk, Trust and Usefulness for Privacy Protection, it seems to be a core construct in the perception of privacy-enhancing features of the Privacy-ABC system, which is a reasonable outcome.

Surprisingly, Understanding of the technology seems not to play an important role in user acceptance (H16 rejected). Moreover, Understanding is not correlated to any of the considered constructs. Below we discuss this unexpected result in more detail.

6.2 Insights into the Understanding of Privacy-ABCs

Apart from being hypothesized as important for user acceptance, understanding of the principles behind the Privacy-ABC technology is of independent interest. For example, it might provide an upper bound on the ability of non-specialists to understand Privacy-ABCs, as the participants in the Patras trial have high technical literacy and were given an introductory lecture on the topic. Moreover, knowing which concepts are understandable and which are not may inform the future interface design, such that

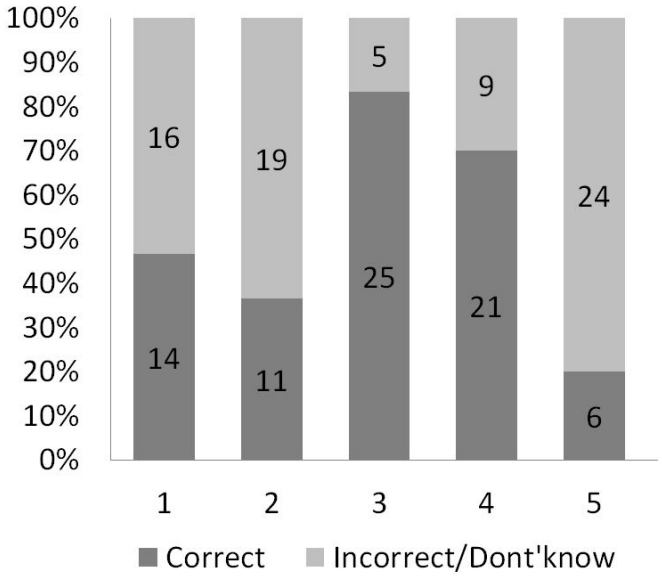

Figure 7: Answers of the trial participants to the five questions about the properties of Privacy-ABCs.

more emphasis should be placed on clear communication of the less understandable features of the Privacy-ABC technology. Thus, we first discuss the overall understanding of the technology by participants, and then consider the absence of correlations between Understanding and any other variables.

We measured how well the participants understand the concepts behind the Privacy-ABCs by means of a new index consisting of five statements that could be rated as true or false, with the "don't know" answer option also available:

1. When I authenticate to the Course Evaluation System (called CES in the following), the smart card transmits my matriculation number to the CES. **(false)**

2. When I authenticate to the CES, the smart card transmits the number of my class attendances to the CES. **(false)**

3. When I evaluate the same course for the second time, the CES does not recognize that I have already evaluated the course. My first evaluation and my second evaluation are seen as evaluations by different students by the CES. **(false)**

4. When I evaluate the same course for the second time, the CES knows that I have already evaluated the course, but it is still not able to identify me. **(true)**

5. When I access the CES from a PC, Privacy-ABCs anonymize my IP address. **(false)**

Question 1 refers to the *pseudonymity* of the Privacy-ABC transactions: a matriculation number is an identifying piece of information, thus it cannot be transmitted during a course evaluation. Only half of the participants answered this question correctly (see Fig. 7).

Only one third of the users correctly answered question 2. It refers to the *minimal disclosure* property: the number of class attendances is an unnecessarily detailed information that can even be used for de-anonymization. Actually, only a boolean value is transmitted that indicates whether the student attended enough lectures in order to be entitled to course evaluation.

Questions 3 and 4 concern the *consumption control* and the *unlinkability* properties: on the one hand, the opinion of the same person cannot be counted twice, and on the other hand, two course evaluations by the same person cannot be used for de-anonymization of this person. Most students were able to understand these facts, probably because these properties are to be expected from any "normal" course evaluation system.

Question 5 refers to the property of network anonymity. This property should be guaranteed on the network layer, and thus, the Privacy-ABC system actually does not possess it. The fact that most of the students thought otherwise gives a clue for the future implementations of Privacy-ABCs: the network anonymity property should either be satisfied, or the implementation should make clear that the protection given by Privacy-ABCs has certain limits.

On the whole, the understanding of Privacy-ABCs seems to be insufficient and difficult to achieve. Probably better understanding can be achieved by specially designed user interfaces, as suggested by Wästlund et al. [51].

Considering the absent correlations between Understanding and any other variables, combined with the prominent misunderstanding of the most important Privacy-ABCs properties (pseudonymity and minimal data disclosure) and a high level of user acceptance, gives a rather hopeless picture for the ability of the users to rationally reason about the important security- and privacy-related properties of a system and base their choice on this reasoning. This does not come as a surprise, however. Impediments to rational reasoning in the privacy matters are well known in the behavioral economics [4].

Especially bounded rationality seems to play and important role here: Although the users were informed about the properties of the system in an introductory lecture, they were probably unable to fully process this information, especially as it contained the new paradigm of data minimization. This corresponds to the experience reported by Harbach et al. [24] about their interviews with German citizens on the topic of privacy-preserving authentication services of the new German identity card. In the focus groups that they conducted, they first explained the properties of the cards, including pseudonymity and data minimization, only to notice that the discussions of the participants never included these properties but concentrated on other issues instead: "The nPA's eID functionality was mostly reduced to how ID cards are currently used and especially the privacy-preserving pseudonymous identification functionality was quickly forgotten during the discussion" [24, p. 13].

7 Trade-offs in the Patras Trial

The calculation of the expected payoff of completing the transaction, as presented in Section 3.3 in Equation 1 (page 9) from the data of a real-world trial can be useful in several ways. For example, one could compare utilities of users that conduct the same transaction by means of different PETs in order to understand which technology has better chances to be adopted. Furthermore, one could probably understand the difference between adopters and non-adopters of concrete PETs in more detail. Although the structure of the Patras trial does not allow for the above comparisons, we use the trial as a case study for the feasibility of such calculations and their shortcomings.

How can we apply the framework of Equation 1 to the concrete situation of course evaluation using the Privacy-ABC technology? One possibility is to consider *subjective* payoffs and probabilities in the Equation 1, such as considered by Acquisti et al. [3] in the analysis of the incentives to participate in distributed anonymity systems. Then the resulting utility can be represented in a simplified form:

$$u_t = v_E(t)p^d(t) + v_E(a)p^d(a) - c_t^d \tag{2}$$

where t is the course evaluation, and d is the Privacy-ABC technology.

We still cannot calculate the above utility using the data from the trial, as, for example, we do not know the probabilities $p^d(t)$ and $p^d(a)$. It could be possible, however, to approximate the Equation 2 using our data, as shown below.

Payoffs of Privacy-ABCs Usage in Course Evaluation The terms $v_E(t)$ and $v_E(a)$ in equation 2 can be considered as the technology-independent subjective valuation that the users assign to the evaluation of a course and to the keeping of anonymity during this evaluation. We can use the answers to the following survey questions to estimate the valuations (both answered on a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree"):

- I_{CE}: Participating in course evaluations is important to me.
- I_A: It is important to me to protect my anonymity when participating in course evaluations.

The subjective probabilities $p^d(t)$ of completing the course evaluation using Privacy-ABCs and $p^d(a)$ of retaining anonymity in the evaluation process can be estimated by considering Perceived Usefulness for Primary Task (PU1) and Perceived Usefulness for Secondary Task (PU2). Although PU1 and PU2 do not measure probabilities, they can be considered as measuring the subjective estimations of the successful completion of the respective tasks. Therefore, we estimate the benefits b_t^d of the Patras trial for each participant as follows, normalized such that the values of b_t^d fall into the interval [1...5]:

$$b_t^d = \frac{I_{CE}PU1 + I_APU2}{12} + \frac{5}{6} \tag{3}$$

This calculation is controversial, however. As Davis a et al. argue [16, p. 988], multiplying scales that are not at the ratio level of measurement can be problematic, as it introduces a systematic error of unknown magnitude. Moreover, Perceived Usefulness may be unsuitable for task success estimation. And finally, as PEoU in the classical TAM usually has a quite strong effect on PU (we can also observe this in our model on the basis of the highly significant correlation with large effect size between PU1 and PEoU), Davis [15, p. 483] argues that the Perceived Usefulness construct may reflect not only benefits, but also costs, these costs being the usage effort that is the opposite of PEoU.

Cost factor	**Definition**	m	σ
Mental effort	Interaction with the system requires a lot of mental effort	2.20	.85
Physical effort	Interaction with the system takes too much time for executing manual operations (clicks, data input, handling the smart card)	2.60	.97
Learnability effort	Usage of the system is difficult to learn	2.40	.81
Memorability effort	Remembering how to interact with the system is difficult	3.33	.99
Low helpfulness	Help information provided by the the system is not effective	1.93	.69
Error recovery effort	Mistakes made during the system usage are difficult to correct	2.57	.97
Worries about smartcard loss	User feels anxious about the possibility of losing the smartcard	2.23	1.22
Worries about data storage	User feels uncomfortable knowing that his/her personal data is stored on a smartcard	2.30	.95

Table 3: Usability costs of the Privacy-ABCs usage, rated from 1 = "strongly disagree" to 5 = "strongly agree", m = mean value, σ = standard deviation. As the statements were formulated negatively, lower scores indicate better usability.

Costs of Privacy-ABCs Usage in Course Evaluation There are at least two possibilities to consider the costs of Privacy-ABCs usage c_t^d:

- the reversed values of Perceived Ease of Use (PEoU), i.e., if a participant's PEoU value was $x \in [1..5]$, then $c_t^d = 6 - x$;
- the direct estimation of the usability costs from the survey, where we asked several usability questions that are presented below.

We compiled a list of usability indicators from classical usability definitions (Nielsen [35] and Quesenbery [39]), long-standing and extensively validated usability scales (Lewis [28] and Brooke [10]), with the aid of a PET-specific, but unfortunately scarcely validated scale by Wästlund et al. [53].

With the help of these indicators, we can examine the usability costs in more detail. We asked the participants to rate statements (from 1 = "strongly disagree" to 5 =

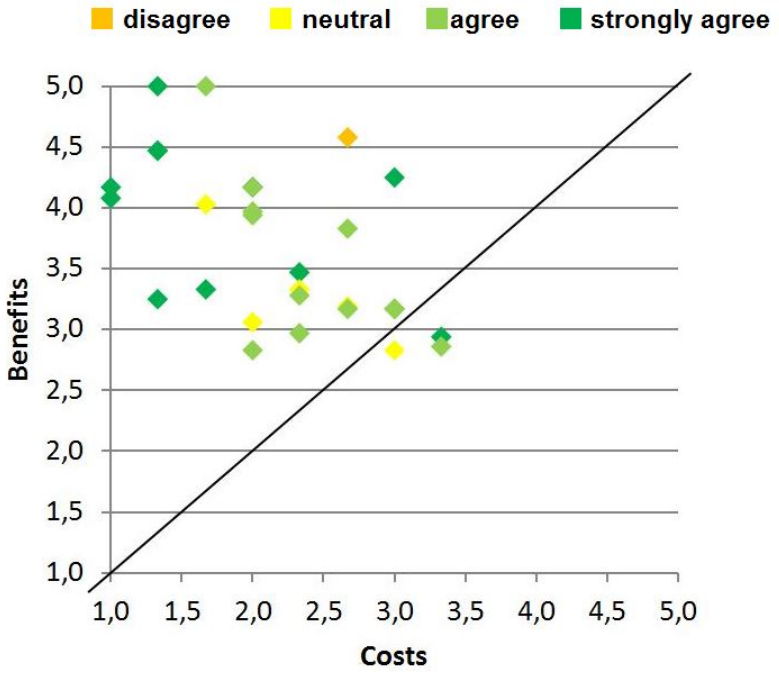

Figure 8: Cost-benefit relation for the usage of Privacy-ABCs in the Patras Pilot; In the plot, for each participant a single point expresses the individual calculated cost-benefit relation, with the value for costs depicted on the X-axis, and the value of benefits depicted on the Y-axis. The direct cost-benefit assessment shows participant's rating of the statement "I find that the benefits of using the Privacy-ABC system are bigger than the effort to use it".

"strongly agree") about concrete usability costs of the system. The definitions of the cost indicators are presented in Table 3.

There is a highly significant medium size correlation ($\tau = 487, p = .000$) between the reversed PEoU and the usability costs computed as an average of the ratings for the usability costs questions in the survey. This serves as an additional indicator that the reversed Perceived Ease of Use can be taken as an estimate of usability costs.

The plot of the resulting cost-benefit relation is presented in Fig. 8. We note, however, that these estimations do not fit well the direct cost-benefit estimations in the trial. Our questionnaire also directly asked the participants to rate (from 1 = "strongly disagree" to 5 = "strongly agree") the statement "I find that the benefits of using the Privacy-ABC system are bigger than the effort to use it". As can be seen in Fig. 8, the comparison of the direct and calculated cost-benefit estimation is not very accurate. Thus, the calculation of the trade-offs and their fit with the direct trade-off estimation remains an open question.

8 Discussion

How accurate is our TAM extension? One possible verification of our results is represented by an independently and concurrently conducted qualitative study of Harbach et al. [24] on the user acceptance of the privacy-preserving authentication of German national identity cards. The authors identify barrier factors for adoption of eID authentication that seem to be reasonably well connected to the reversed factors of user acceptance that we found:

- No added value (users do not see any benefits in using the eID authentication) is a counterpart to PU1, as no compelling applications were known to the users. The authors of the study comment that the users do not see how the eID authentication can make their life easier.
- Complexity (users perceive the additional eID features as too complex) is reversed PEoU.
- Fear of control loss (user fear that the system might do something unexpected, cannot be sure which information is actually transmitted) is connected to the reversed Situation Awareness and Trust.
- No security benefit (users report that they don't see additional eID security as a benefit) can be considered as the negative counterpart of PU2, as the users do not see how eID authentication can contribute to their online security.
- Poor understanding of privacy-preserving pseudonymous authentication that was noticed in the conducted focus groups directly confirms our findings.

Some additional barrier factors were also identified in [24], such as additional cost (users of eIDs would have to buy a smart card reader) and insufficient information about the additional eID features at the public service offices.

What is Needed for the Acceptance of PETs? According to the conventional wisdom, in order to adopt PETs, people need to understand their benefits. It is also often assumed that risk perception is connected to the understanding of privacy risks. The reasoning is that if the users would perceive risk for their privacy as high, and the efficacy of PETs in reducing this risk as high, then they would adopt PETs. However, we see a different picture in our trial. Although the participants did not understand the properties of Privacy-ABCs well, they felt well protected, and the perception of the overall system as useful for the primary task was strongly correlated with high user acceptance.

Considering our results, it seems that integration of sophisticated PETs into systems and products should be driven by political, legal and ethical considerations, not by user demand, as there are too many impediments for the latter. These impediments are well known from the behavioral economics: incomplete information, bounded rationality

and behavioral biases [4]. Most importantly, users would only adopt PETs that are integrated into useful services. In this case, we think that people may accept some usability drawbacks that arise from the PET integration, such as having to use a smart card or to consult a user manual sometimes. Although good usability and usefulness for privacy protection are important factors of user acceptance, our empirical results indicate that perceived usefulness of the primary (not privacy-related) service is much more important.

Limitations The results and conclusions from the Patras Pilot have to be further verified in other studies, as our trial had a lot of limitations that might have influenced the results. For example, users that found Privacy-ABCs inconvenient or untrustworthy could have refused to participate (so-called self-selection bias), such that we were unable to investigate their opinions and technology rejection factors. Furthermore, the trustworthy university environment could have increased trust into the system, and thus also the perceived usefulness for privacy protection. Moreover, computer science students are more likely to be early adopters, which could imply exaggerated user acceptance results in comparison to the general population. Also good usability results may have been positively influenced by the high technical literacy of the users.

9 Conclusion

In this work, we extended the Technology Acceptance Model for the evaluation of user acceptance of privacy-enhancing technologies. We introduced five new constructs into the TAM: Perceived Usefulness for the Primary Task (PU1), Perceived Usefulness for the Secondary Task (PU2), Situation Awareness, Perceived Anonymity and Understanding of the PET. We conducted a preliminary evaluation of our model in the concrete scenario of a university course evaluation. The tentative conclusions from our study indicate that PU1 is the most important factor of user adoption, outweighing the usability and the usefulness of the deployed PET (PU2). Moreover, correct Understanding of the underlying PET seems to play a much less important role than a user interface of the system that clearly conveys to the user which data are transmitted when and to which party (Situation Awareness).

Unfortunately, the sample size (30 participants) is prohibitively small for deeper statistical analysis such as multiple regressions or structural equation modeling, such that a more rigorous validation of the model, as well as further considerations on the calculations of PET usage trade-offs from the data of real-world trials, are left to future work.

Acknowledgments We thank the ABC4Trust team of the Patras University, consisting of Vasiliki Liagkou, Apostolos Pyrgelis and Yannis Stamatiou, for their awesome support in the practical realization of the survey during the trial. We thank Vasiliki Liagkou and Welderufael Tesfay for many fruitful discussions on the adaptation of the scales. We are also very grateful to the anonymous reviewers for their insightful and

extremely helpful comments. Zinaida Benenson and Anna Girard were supported by the Bavarian State Ministry of Education, Science and the Arts as part of the FORSEC research association.

References

[1] Alessandro Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*, pages 21–29. ACM, 2004.

[2] Alessandro Acquisti. The economics of personal data and the economics of privacy. *Background Paper for OECD Joint WPISP-WPIE Roundtable*, 1, 2010.

[3] Alessandro Acquisti, Roger Dingledine, and Paul Syverson. On the economics of anonymity. In *Financial Cryptography*, pages 84–102. Springer, 2003.

[4] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 2:24–30, 2005.

[5] Zinaida Benenson, Anna Girard, Ioannis Krontiris, Vassia Liagkou, Kai Rannenberg, and Yannis Stamatiou. User acceptance of Privacy-ABCs: An exploratory study. In *HCI International: Human Aspects of Information Security, Privacy and Trust*, 2014.

[6] Yoav Benjamini and Yosef Hochberg. Controlling the false discovery rate: a practical and powerful approach to multiple testing. *Journal of the Royal Statistical Society. Series B (Methodological)*, pages 289–300, 1995.

[7] Ronny Bjones, Ioannis Krontiris, Pascal Paillier, and Kai Rannenberg. Integrating anonymous credentials with eIDs for privacy-respecting online authentication. In *Privacy Technologies and Policy*, pages 111–124. Springer, 2014.

[8] Anick Bosmans and Hans Baumgartner. Goal-relevant emotional information: When extraneous affect leads to persuasion and when it does not. *Journal of Consumer Research*, 32(3):424–434, 2005.

[9] Stefan A. Brands. *Rethinking public key infrastructures and digital certificates: building in privacy.* The MIT Press, 2000.

[10] John Brooke. SUS - A quick and dirty usability scale. *Usability evaluation in industry*, 189:194, 1996.

[11] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology–EUROCRYPT 2001*. Springer, 2001.

[12] Jan Camenisch and Els Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 21–30. ACM, 2002.

[13] Jacob Cohen. *Statistical power analysis for the behavioral sciences*. Lawrence Erlbaum Associates, Inc, 1988.

[14] Fred D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[15] Fred D. Davis. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, 38(3):475–487, 1993.

[16] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8):982–1003, 1989.

[17] Tamara Dinev and Paul Hart. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1):61–80, 2006.

[18] Tamara Dinev and Paul Hart. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2):7–29, 2006.

[19] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. G* power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods*, 39(2):175–191, 2007.

[20] Andy Field. *Discovering statistics using IBM SPSS statistics*. Sage, 2013.

[21] Final Report to the European Commission DG Justice, Freedom and Security. Study on the economic benefits of privacy-enhancing technologies (PETs). Technical report, London Economics, July 2010.

[22] Andrew Gelman, Jennifer Hill, and Masanao Yajima. Why we (usually) don't have to worry about multiple comparisons. *Journal of Research on Educational Effectiveness*, 5(2):189–211, 2012.

[23] Cornelia Graf, Peter Wolkerstorfer, Christina Hochleitner, Erir Wästlund, and Manfred Tscheligi. HCI for PrimeLife Prototypes. In Jan Camenisch, Simone Fischer-Hübner, and Kai Rannenberg, editors, *Privacy and Identity Management for Life*, chapter 11, pages 221–232. Springer, 2011.

[24] Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith. On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In *Privacy Enhancing Technologies*, pages 245–264. Springer, 2013.

[25] Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur, and H Raghav Rao. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, 24(1):61–84, 2014.

[26] Younghwa Lee and Kenneth A. Kozar. Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, 48(8):72–77, 2005.

[27] Younghwa Lee and Kenneth A. Kozar. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Inf. Manage.*, 45(2):109–119, March 2008.

[28] James R. Lewis. IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use. *International Journal of Human-Computer Interaction*, 7(1):57–78, 1995.

[29] Celia M. Lombardi and Stuart H. Hurlbert. Misprescription and misuse of one-tailed tests. *Austral Ecology*, 34(4):447–468, 2009.

[30] Carolina Martins, Tiago Oliveira, and Aleš Popovič. Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34(1):1–13, 2014.

[31] D. Harrison McKnight, Michelle Carter, Jason Bennett Thatcher, and Paul F. Clay. Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, 2(2):12, 2011.

[32] Microsoft Research. U-Prove: `http://research.microsoft.com/en-us/projects/u-prove`.

[33] Jian Mou and Jason F. Cohen. Trust and risk in consumer acceptance of e-services: A meta-analysis and a test of competing models. In Richard Baskerville and Michael Chau, editors, *Proceedings of the International Conference on Information Systems, ICIS 2013, Milano, Italy, December 15-18, 2013*. Association for Information Systems, 2013.

[34] Shinichi Nakagawa. A farewell to Bonferroni: the problems of low statistical power and publication bias. *Behavioral Ecology*, 15(6):1044–1045, 2004.

[35] Jakob Nielsen. *Usability engineering*. Elsevier, 1994.

[36] Paul A. Pavlou. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, 7(3):101–134, 2003.

[37] John Sören Pettersson, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Kriegelstein, and Henry Krasemann. Making PRIME usable. In *Proceedings of the 2005 symposium on Usable privacy and security*, pages 53–64. ACM, 2005.

[38] Andreas Poller, Ulrich Waldmann, Sven Vowé, and Sven Türpe. Electronic identity cards for user authentication – promise and practice. *IEEE Security & Privacy*, 10(1):46–54, 2012.

[39] Whitney Quesenbery. The five dimensions of usability. *Content and complexity: Information design in technical communication*, pages 81–102, 2003.

[40] Graeme D. Ruxton and Markus Neuhäuser. When should we use one-tailed hypothesis testing? *Methods in Ecology and Evolution*, 1(2):114–117, 2010.

[41] Sarah Spiekermann. *User control in ubiquitous computing: design alternatives and user acceptance*. Shaker, 2008.

[42] Sarah Spiekermann and Lorrie Faith Cranor. Engineering privacy. *Software Engineering, IEEE Transactions on*, 35(1), 2009.

[43] Yannis Stamatiou, Zinaida Benenson, Anna Girard, Ioannis Krontiris, Vasiliki Liagkou, Apostolos Pyrgelis, and Welderufael Tesfay. Course evaluation in higher education: the Patras pilot of ABC4Trust. In *Attribute-based Credentials for Trust*, pages 197–239. Springer, 2015.

[44] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. What makes users refuse web single sign-on?: an empirical investigation of OpenID. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 4. ACM, 2011.

[45] Viswanath Venkatesh and Hillol Bala. Technology acceptance model 3 and a research agenda on interventions. *Decision sciences*, 39(2):273–315, 2008.

[46] Viswanath Venkatesh and Fred D. Davis. A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management science*, 46(2):186–204, 2000.

[47] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. User acceptance of information technology: Toward a unified view. *MIS quarterly*, pages 425–478, 2003.

[48] Viswanath Venkatesh, James Y.L. Thong, and Xin Xu. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 36(1):157–178, 2012.

[49] Paul R. Warshaw and Fred D. Davis. Disentangling behavioral intention and behavioral expectation. *Journal of experimental social psychology*, 21(3):213–228, 1985.

[50] Rick Wash and Emilee Rader. Influencing mental models of security: a research agenda. In *New security paradigms workshop*, pages 57–66. ACM, 2011.

[51] Erik Wästlund, Julio Angulo, and Simone Fischer-Hübner. Evoking comprehensive mental models of anonymous credentials. In *Open Problems in Network Security*, pages 1–14. Springer, 2012.

[52] Erik Wästlund and Simone Fischer-Hübner. The users' mental models' effect on their comprehension of anonymous credentials. In Jan Camenisch, Simone Fischer-Hübner, and Kai Rannenberg, editors, *Privacy and Identity Management for Life*, chapter 12, pages 233–244. Springer, 2011.

[53] Erik Wästlund, Peter Wolkerstorfer, and Christina Köffel. PET-USES: Privacy-enhancing technology – users self-estimation scale. In *Privacy and Identity Management for Life*, pages 266–274. Springer, 2010.

A Quality Criteria for Scales

Regarding the quality criteria, we evaluated the convergent validity of our scales with separate principal component analysis (PCA) with Varimax rotation, in order to prove one-dimensionality for every construct as suggested by (Homburg and Giering, 1996). We also checked for reliability and internal consistency of measurements. We had to drop one item of the original ease of use scale which did not exceed the quality criteria; all other scales remained unchanged. For the PCA, the Bartlett test indicated significant correlations for all constructs, the Kaiser-Meyer-Olkin (KMO) measure verified the sampling adequacy for the analysis with at least KMO = .595, and all measures of sampling adequacy (MSA) values for individual items were greater or equal than .559. Thus, KMO and MSA exceed the acceptable limit of .500 (Field, 2013). All constructs showed only one factor with an eigenvalue greater than one, which explained at least 57% of the variance (should exceed at least 50%) and factor loadings greater or equal to .661 (should be greater than .400) (Backhaus, 2003; Homburg and Giering, 1996).

Both Cronbach's α which should exceed .700 ($\geq$ .774) as well as the item-to-total correlation which should be above .500 ($\geq$ .541) militate in favor of high reliability and internal consistency of our measurements (Field, 2013; Homburg and Giering; 1996). Exact results of the analysis are presented in Table 4 on page 33.

- Backhaus, K. (2003), Multivariate Analysemethoden - eine anwendungsorientierte Einführung, Springer, Berlin.
- Field, A. (2013), Discovering Statistics Using IBM SPSS Statistics, SAGE Publications, London.
- Homburg, C. & Giering, A. (1996), *Konzeptualisierung und Operationalisierung Komplexer Konstrukte: Ein Leitfaden für die Marketingforschung.* Marketing: Zeitschrift für Forschung und Praxis, Vol. 18, No. 1, pp. 5-24.

	Factor loading	KMO	Bartlett sig.	MSA	Variance explained	Cron-bach's α	Item to Total
Intention to Use (adapted from [46, 45])		.698	.000		88.69%	.936	
Assuming that the Privacy-ABC system is available for course evaluations, I intend to use it.	.905			.834			.798
I would use the Privacy-ABC system for course evaluations in the next semester if it is available.	.947			.683			.876
Given that the Privacy-ABC system is available for course evaluations, I would use it.	.971			.628			.931
Perceived Usefulness for Primary Task (adapted from [46, 45])		.737	.000		83.81%	.903	
Using Privacy-ABCs improves the performance of course evaluation.	.938			.685			.851
Using Privacy-ABCs enhances the effectiveness of course evaluation.	.903			.773			.786
I find Privacy-ABCs to be useful for course evaluation.	.905			.767			.788
Perceived Usefulness for Secondary Task (adapted from [46, 45])		.770	.000		90.44%	.947	
Using Privacy-ABCs improves my privacy protection.	.959			.732			.906
Using Privacy-ABCs enhances the effectiveness of my privacy protection.	.948			.782			.884
I find Privacy-ABCs to be useful in protecting my privacy.	.945			.799			.877
Perceived Ease of Use (adapted from [46, 45])		.732	.000		77.59%	.853	
Interacting with the Privacy-ABC System does not require a lot of my mental effort.	.888			.718			.740
The Privacy-ABC System is easy to use.	.886			.722			.737
I find it easy to get the Privacy-ABC System to do what I want to do.	.868			.760			.706
Perceived Anonymity (adapted from [8])		.595	.000		71.38%	.774	
Privacy-ABCs are able to protect my anonymity in course evaluation.	.826			.607			.570
With Privacy-ABCs I obtain a sense of anonymity in course evaluation.	.925			.559			.779
Privacy-ABCs can prevent threats to my anonymity in course evaluation.	.777			.647			.542
Situation Awareness (adapted from [53])		.774	.000		56.66%	.868	
With Privacy-ABCs, I always know which personal information I am disclosing.	.806			.833			.709
I find it easy to see which information will be disclosed in order to get a credential.	.869			.695			.799
Privacy-ABCs let me know who receives my data.	.766			.917			.664
The Privacy-ABC system gives me a good overview of my personal data stored on my Smart Card.	.707			.654			.584
I can easily find out when (e.g., at which date) I have received a credential via the University Registration System.	.661			.863			.541
I get a good overview of who knows what about my private information from the Privacy-ABC System.	.668			.737			.555
I can easily see which and how many Privacy-ABC credentials I have been issued.	.770			.807			.674

Table 4: Quality criteria for measurement scales for the adapted TAM; all items are measured on a 5-point scale ranging from 1 = "strongly disagree" to 5 = "strongly agree". Mean values and standard deviations for the scales are presented in Table 2 on page 18.