D7.3 Evaluation of the Student Pilot

Daniel Deibler, Malte Engeler, Ioannis Krontiris, Anja Lehmann, Vasiliki Liagkou, Apostolos Pyrgelis, Eva Schlehahn, Yannis Stamatiou, Welderufael Tesfay, Harald Zwingelberg

Editors:	Vasiliki Liagkou (CTI)
Reviewers:	Norbert Goetze (NSN), Welderufael Tesfay (GUF)
Identifier:	D7.3
Type:	Deliverable
Version:	1.0
Date:	1/5/2014
Status:	Final
Class:	Public

Abstract

This deliverable is focused on the evaluation results from the first and second rounds of the pilot conducted within the scope of WP7 of the project. The document reports and discusses the general feedback of the pilot participants (students) with respect to the usability and effectiveness of Privacy-ABC technologies in preserving their privacy while they interact with electronic services. The evaluation results are analyzed with both quantitative and qualitative methodologies which we explain in the document.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

Members of the ABC4TRUST Consortium

1.	Alexandra Institute A/S	ALX	Denmark
2.	CryptoExperts SAS	CRX	France
3.	Eurodocs AB	EDOC	Sweden
4.	IBM Research – Zurich	IBM	Switzerland
5.	Johann Wolfgang Goethe – Universität Frankfurt	GUF	Germany
6.	Microsoft Research and Development	MS	France
7.	Miracle A/S	MCL	Denmark
8.	Nokia Solutions and Networks GmbH & Co. KG	NSN	Germany
9.	Research Academic Computer Technology Institute	CTI	Greece
10.	Söderhamn Kommun	SK	Sweden
11.	Technische Universität Darmstadt	TUD	Germany
12.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany

List of Contributors

Chapter	Author(s)
0. Executive Summary	Yannis Stamatiou (CTI)
1. Introduction	Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI)
2. Pilot's Scenarios	Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI)
3. Evaluation of the Student Pilot's Components	Daniel Deibler (ULD), Malte Engeler (ULD), Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI), Eva Schlehahn (ULD), Harald Zwingelberg (ULD)
4. User Acceptance of Privacy-ABCs	Ioannis Krontiris (GUF), Vasiliki Liagkou(CTI), Welderufael Tesfay (GUF)
5. Legal Considerations	Malte Engeler (ULD), Daniel Deibler (ULD), Vasiliki Liagkou (CTI), Eva Schlehahn (ULD), Yannis Stamatiou (CTI), Harald Zwingelberg (ULD)
6. Recommendations	Daniel Deibler (ULD), Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI), Yannis Stamatiou (CTI),
Appendix A	Malte Engeler (ULD), Vasiliki Liagkou (CTI), Eva Schlehahn (ULD), Harald Zwingelberg(ULD)
Appendix B	Malte Engeler (ULD), Vasiliki Liagkou (CTI), Eva Schlehahn (ULD), Harald Zwingelberg (ULD)
Appendix C	Malte Engeler (ULD), Vasiliki Liagkou (CTI), Eva Schlehahn (ULD), Harald Zwingelberg (ULD)
Appendix D	Vasiliki Liagkou (CTI)
Appendix E	Vasiliki Liagkou (CTI)
Appendix F	Anja Lehmann (IBM), Apostolos Pyrgelis (CTI)
7. Bibliography	Vasiliki Liagkou (CTI)

Executive Summary

This deliverable is focused on the description and analysis of the User evaluation results from the first and second rounds of the Patras pilot conducted within the scope of WP7 of the project. The goal of this pilot is to employ Privacy-ABCs into a course evaluation application that allows only eligible university students to evaluate, anonymously, courses they have attended throughout the semester. The design, implementation, and testing of the pilot system was based on the use cases, pilot requirements, and pilot system architecture documented in deliverable D5.1, D7.1, and D7.2 respectively.

Moreover, while the implementation of the pilot systems of the first round was based on the first version of the reference implementation provided by WP4, the second round of the pilot was based on the new crypto architecture. This new architecture contains a number of improvements and new features over the first version of the architecture including carry-over attributes and the interoperability between U-prove and Idemix technologies.

In this document we briefly discuss the timeline and content of the two rounds of the student pilot as well as the relevant documentation (legal documents and student questionnaires, which are placed in the appendices). We then discuss the pilot scenarios in detail and show how they are related to the evaluation process. We also discuss the success criteria of the pilot, as documented in D5.1, and the degree to which the realization of the two rounds met these criteria.

We then proceed to describe the findings of the evaluation of the pilot. The main focus of this deliverable is on the Users' side and, more specifically, it presents the opinions of the participants towards the pilot system as well as the Privacy-ABCs' concepts and technologies. In order to obtain the student's opinions, we designed suitable questionnaires that were given out to students after the course evaluation period was over, near the end of the semester. Their completed questionnaires were collected, anonymously, and were then subjected to quantitative and qualitative analysis. In the deliverable we explain the methodology that we followed in developing and analyzing the questionnaires and provide graphs of the quantitative results that show the overall impressions of the participating students towards the Privacy-ABC technologies.

In summary, the evaluation's conclusion was that the students feel that Privacy-ABCs form an important technology that can help them manage their e-Identities and enable them to use Internet services in a privacy preserving way. Most of them felt assured, during the pilot's run, that their privacy was not violated while they were interacting with the pilot system using their smart cards and credentials and the found the systems' responsiveness and speed good.

Table of Contents

Index of Figures

Index of Tables

1 Introduction

In this chapter we give a brief description of the two rounds of the student pilot (see deliverables D7.1 [ADFS12] and D7.2 [NHSPSPD] for more details). Moreover, we present the scope and the structure of this document.

1.1 A Brief Account of the Two Pilot Rounds

The pilot took place at the Computer Engineering and Informatics Department of the University of Patras in Greece (CEID). It consisted of two rounds where the first round was run with the first version of the reference implementation, while the second round (which began on the 15th of October 2013) tested an enhanced version with additional functionality. All the students were able to access the pilot systems at any time from their homes, as well as (if necessary) from a specific personal computer located at CTI's premises which was equipped with smart card readers and the Application.

All the participating students of the first and the second round of student pilot used the Privacy-ABC technologies for the evaluation of the "Distributed Systems I" course. This course is a non-compulsory course that takes place at the 7th semester and the number of students that attended it was approximately 60 in both pilot rounds. The lectures for the course took place at the B4 lecture room in B Building which is the main building of the Computer Engineering and Informatics Department (Figure 1 and Figure 5 show the classroom for the two semesters). CTI, together with the help of teaching assistants, placed a Near Field Communication (NFC contactless) reader in the lecture room prior to each lecture.

1.1.1 The First Round of Pilot

Before the start of the first round, a thorough on-site testing of the pilot system was conducted. The on-site testing started on May 2012. Three CTI members and 6 students participated in the testing phase. We had a thorough list of test cases that helped us deliver a stable system to the Users. The CTI members realized the list of the test cases using Privacy-ABCs without smart cards (SCs). In October 2012, 6 students/volunteers took part in the testing phase using their SCs. The testing phase checked the main pilot system functionalities, as well as some preliminary crypto features of the reference architecture that were not deployed during the first round, e.g., generation of proofs requiring a combination of credentials.

For the first round of student pilot, two groups of students took part in the evaluation. Initially, a group of 32 students was formed in order to evaluate the course by using the Idemix technology. We planned for the second group of 16 students to evaluate the course by using the U-Prove technology, but unfortunately the reference implementation was not mature enough to support U-Prove technology adequately in the first round of the student pilot. Due to this fact, all of the 48 students evaluated the course using the Idemix implementation, while 7 of the 48 students evaluated the course, near the end of the semester, using both U-Prove and Idemix technologies.

All of the 48 participating students took the following actions, in sequence, in order to evaluate the course in a way that both ensured the credibility of results and preserved the privacy of the students expressing their opinion:

1. All of the participating students had an Idemix smart card in their possession, while six of them were also equipped with a U-Prove smart card.
2. As a first step, they registered their smart card.
3. After this registration step, the students were able to obtain their credentials from the University Registration System.

4. All the students collected their attendance units at each lecture in the B4 lecture room of the CEID building.
5. Each student could make a backup of her attendance units, as well as restore the backed up data on a new SC (e.g. in the case of SC loss).
6. In order to submit their course evaluation, students had to prove that: i) they were registered to the course under evaluation, and ii) they attended a sufficient number of lectures.

It was important for the student pilot's success to get some preliminary feedback from students and professors on privacy-respecting online course evaluation processes. We distributed questionnaires through which the opinions of the students and professors were collected and analyzed with respect to several criteria pertaining to the Privacy-ABCs concept, as well as regarding the reference implementation that the students used during the first round of the pilot.

We developed two questionnaires for the first round of the student pilot and then analyzed the produced results:

- The first questionnaire was distributed before the first round of the student pilot took place and before students were informed, in depth, about Privacy-ABCs technologies. These questionnaires were included in D7.1 (see [ADFS12]) and they were composed of questions that were targeted to address the students' feelings towards electronic evaluation procedures as compared to the traditional ones they might have already participated in. This first feedback from students and professors was presented also in D7.1 (see [ADFS12]) and was used as a guideline in order to adjust the student pilot according to the needs of the students and the professors.
- The second questionnaire was distributed after the first round when the course evaluation had already taken place. The questionnaire is presented in the Appendix (see Appendix D) and it contains questions about students' knowledge on Privacy-ABC technologies, the User acceptance and participation of the student pilot acceptance and the usability of the Privacy-ABC technologies. The questionnaires were distributed to all the students who took part in the presentations and demonstrations of the Privacy-ABC technologies. Moreover, the 7 students who took part in the first round of course evaluation using both Privacy-ABC technologies, were presented with an additional questionnaire that addressed the comparison between the two technologies (this questionnaire is presented in Appendix E). These 7 students participated in the course evaluation using the Idemix technology and evaluated the course using, also, U-prove technology for comparison purposes. However, the Course Evaluation system did not take into account the second evaluation of these 7 students.

1.1.1.1 Timeline of the First Round of the Pilot

More specifically, the timeline of the first round of the student pilot included the following steps and actions:

- On September 24, 2012, the course of "Distributed Systems I" started.
- On October 12, 2012, during the lecture, slides were shown introducing the students to the concepts of Privacy-ABCs and the goals of the pilot. The students were briefed in the scope and the goals of the pilot. They were also informed that they could take part, on a volunteer basis, in the first round of the student pilot using Privacy-ABCs. Moreover, at the same time after the lecture, the lecturer and CTI members initiated an open discussion related to the concepts of Privacy-ABCs, the objectives of the project and the scenarios of the pilot. All the students were referred to the pilot's Greek site for more detailed information on their participation in the pilot, as well as the system they will use to participate. The material related to the pilot included the presented slides, the User Manual, links to the Course Evaluation

System (CES) and the IdM Portal and up-to-date information about the status and actions of the student pilot (see Figure 2). Finally, the course instructor added a topic related to the pilot at the discussion forum of the course (see Figure 3). All the notifications and information on the status of ABC4Trust pilot were also available there.

- On October 29, 2012, all the students received the User consent form via email. The interested students were informed that they could participate in the electronic (using Privacy-ABCs) course evaluation in the end of the semester. They were also informed that they should read carefully the User consent form and sign it in order to be able to participate in the pilot. The User consent form was also uploaded on the course's forum.
- On November 2, 2012, during lecture time, demonstration videos were shown introducing the students to the basic actions and functionality of the pilot system. Also, printed consent forms were distributed to students in order to sign them. Then CTI members gathered the signed consent forms and formed the two groups of the volunteer-students. The first group consisted of 32 students and the second one of 16 students.
- On November 23, 2012, during the lecture, each one from the group of the 32 students received:

  - ✓ An Idemix SC.
  - ✓ A contact smart card reader.
  - ✓ An envelope with their PIN and PUK.
  - ✓ A slip of paper containing a one-time-password.

- Moreover, the students collected their first attendance units on their cards using the Class Attendance System that was operated and supervised by CTI senior personnel in the lecture room. Finally, the User Manual and the ABC4Trust software installer were presented to the students. These items were uploaded, later in the day, on the Patras Portal for retrieval by the students. The pilot-relevant personal information of the 32 participating students was obtained via registration sheets directly from the students.
- On 26/11/12, 7/12/12, 10/12/12 and 14/12/12, the 32 participating students collected, again, their attendance units (one per student, per day of attendance). Figure 4 shows the students collecting their attendance units.
- On December 19, 2012 the second group of 16 students was informed that the distribution of the second set of SCs will take place at the first week of January. The date of distribution was announced in the course's forum as well as in the lecture room.
- On January 7 and 9, 2013 at the B4 lecture room in the B Building, the second group of 16 students were informed that they will also use the Idemix technology since the reference implementation could not support U-Prove technology yet. Each one received:

  - ✓ An Idemix SC.
  - ✓ A contact smart card reader.
  - ✓ An envelope with their PIN and PUK.
  - ✓ A slip of paper containing a one-time-password.

Figure 1: Lecture Room of Distributed Systems I at the Fall Semester of 2012

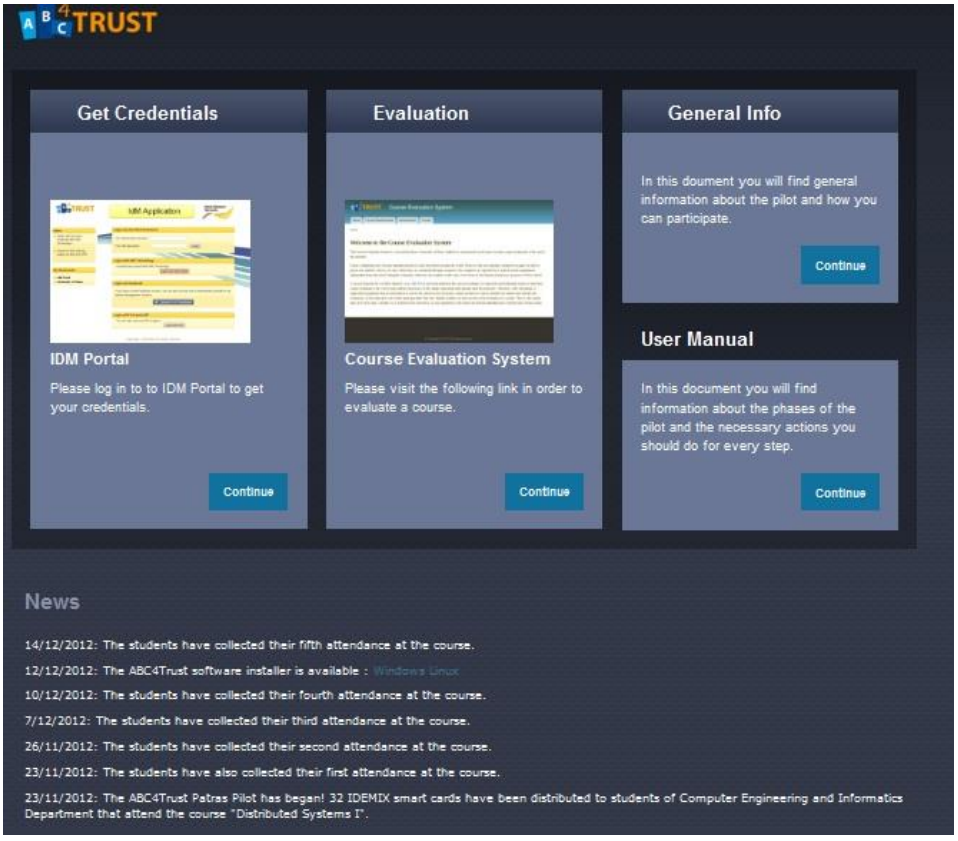


Figure 2: The Patras Portal for the First Round

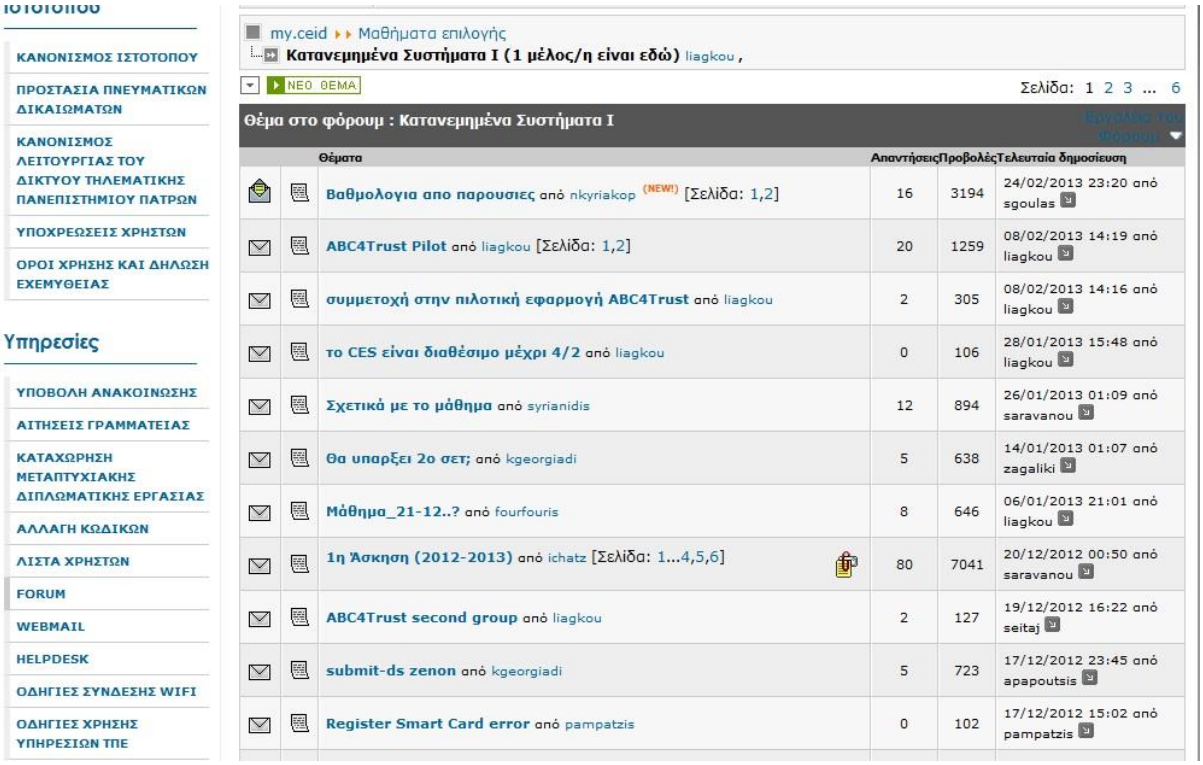


Figure 3: The ABC4Trust Discussion Room at the Course Forum at the Fall Semester of 2012

Figure 4: Students Collecting their Attendance Units for the First Round of the Student Pilot

The second group of students collected their first attendance unit and their pilot relevant personal information was uploaded on the IdM database.

- On January 11, 2013 at the B4 lecture room in CEID Building B, the second group of 16 students collected one more attendance unit. A script program was distributed to the two groups of students, so that all the participated students were able to read their saved attendance units stored on their SCs. Moreover, we changed their threshold value to 1, thus a student

ought to have at least one attendance unit in her smart card in order to be able to participate to the course evaluation.

- On January 20, 2013, the course evaluation system was launched and was accessible online. All the participated students were informed that they could access the Course Evaluation System until the 4th of February. This announcement also appeared on the course forum.
- On January 28, 2013, we reminded the 48 participating students that they should evaluate the course until the 4th of February. Moreover, we informed them that we will distribute the questionnaires at the 5th of February. This information also appeared on the course's forum.
- On February 4, 2013, a 1-week extension was given to all the participating students in order to maximize participation in the evaluation of the course. We also sent them the questionnaires through email in order to give them sufficient time to prepare their responses. More specifically, the students were informed that:

  - ✓ The questionnaires would be distributed at the classroom on 5/2/2013.
  - ✓ Alternatively, they could print the questionnaire, fill in their responses, put it in an envelope and place it in Prof. Yannis Stamatiou's (leader of WP7 of the ABC4Trust project) mailbox at the University of Patras.

  We uploaded this information on the course's forum, too.
- On February 5, 2013, we distributed the printed questionnaires to the students, at the lecture room. A discussion was organized related to the concepts of Privacy-ABCs, the realization of the pilot and the questionnaire.
- CTI, then formed a group of 7 students who participated in the course evaluation using their Idemix SCs and volunteered to evaluate the course using, also, U-Prove SCs for comparison purposes.
- On February 15, 2013, the six volunteers obtained their U-Prove SCs and evaluated the course. The Course Evaluation system did not take into account these six evaluations. They were, also, given an additional questionnaire to complete, focused on the differences between using U-Prove and Idemix SCs.
- On February 16, 2013, the first round of the student pilot ended. All of the distributed questionnaires were gathered and digitally scanned for facilitating reference and analysis.

1.1.2 The Second Round of the Pilot

The second round of the student pilot started in the first month of the fall semester of 2013 targeting again the evaluation of the course "Distributed Systems I", whose final examination was scheduled for the 15th of January 2014. The second round of the student pilot took place between 15th of October 2013 and February 2014. However, the second round of the student pilot included some additional features that are summarized in Section 2.2 and presented in detail in Appendix F. For the second round of the student pilot, a group of 45 students took part in the evaluation. All the participating students could evaluate the course by using both the Idemix and U-Prove technologies. That is, they all received both Idemix and U-Prove credentials and derived presentation tokens based on the combination of both credentials. Moreover, the second round of the Course Evaluation Pilot included some additional features such as revocation and inspection that are presented in Section 2.2 as well.

All of the 45 participating students had in their possession a MultOS smart card, which was compatible with Idemix and U-Prove technologies and they were able to take sequentially the

following actions in order to evaluate the course in a way that both ensures the credibility of results and preserves the privacy of the students expressing their opinion:

1. They could register their smart card.
2. After this registration step, the students were able to obtain their credentials from the University Registration System.
3. All the students collected their attendance units at each lecture in the B4 lecture room.
4. Each student could make a backup of her attendance units as well as restore the backed up data on a new SC (e.g. in the case of SC loss).
5. In order to submit their course evaluation they had to prove that: i) they hold a valid (non-revoked) university credential, ii) they were registered to the course under evaluation, and iii) they attended sufficient number of lectures.
6. After the evaluation step, the students could get a tombola credential in order to be able to take part in a lottery (tombola).

Finally, when the lottery ended, the winner of the lottery game was announced by the Inspector. A student was randomly selected to be the Inspector entity and she announced the winner of the lottery. All the students that took part in the lottery and did not win the prize remained anonymous.

At the second round we updated the formal questionnaires (see Appendix D.1) for collecting opinions of the students so that the questions are more unambiguous and clear. These questionnaires were distributed in order to collect the opinion of the participated students. After the second round of the course evaluation had taken place and the tombola had ended, all the participating students filled out anonymously the printouts of the questionnaire. The questionnaire is presented in the Appendix (see Appendix D.1) and contains questions about the usability of the student pilot, about the new functionalities and features that were included at the second round of the student pilot and about the students' knowledge on Privacy-ABC technologies. The questionnaires were distributed to all 45 participating students who took part in the second round of the student pilot and had received the MultOS smart card.

1.1.2.1 Timeline of the Second Round of the Pilot

The timeline of the second round of the student pilot was similar to the first round and includes the following steps and actions:

- On October 7, 2013 the course of "Distributed Systems I" started. During the lecture, a new updated introductory presentation was shown to the students in order to give an overview of the concepts of Privacy-ABCs and the goals of the pilot. This briefing was similar to the first round and it also introduces the scope, the goals and the new features of the second round of the student pilot.
- On October 14, 2013 the students were informed that they could take part, on a volunteer basis, in the second round of the student pilot using Privacy-ABCs. All the students were informed that the pilot's Greek site is online and it contains all the necessary information for their participation in the second round of the student pilot. The pilot's Greek site included the updated introductory presentation, the new User Manual for the second round of the student pilot, links to the Course Evaluation System (CES), the Tombola System and the IdM Portal, the privacy statement and the up-to-date information about the status and actions of the second round of the student pilot (see Figure 6). Finally, a topic related to the pilot was added at the discussion forum of the course (see Figure 7).
- On October 21 and 28, 2013, during lecture time, demonstration videos were shown introducing the students to the basic actions and functionalities of the second round of student pilot. Also, printed consent forms were distributed to students in order to sign them. After this,

CTI members gathered the signed consent forms and formed a group of 45 students. Our initial plan was to form a group with 30 students.

- On November 4 and on November 11, 2013, the group of the 45 students received the MultOS smart cards and an envelope with their PIN and PUK. Moreover, they collected their attendance units on their cards using the Class Attendance System.
- On November 18, 2013, the group of 45 students received a smart card reader and the one time password in order to register their smart card. Finally, the User Manual and the ABC4Trust software installer were presented to the students. Moreover the ABC4Ttrust User Client Application software was uploaded on the pilot's Greek site.
- On 25/11/13, 2/12/13, 9/12/13 and 16/12/13, the 45 participating students collected, once again, their attendance units (one per student, per day of attendance). Figure 8 shows the students collecting their attendance units. Moreover, all the 45 participating students could view their stored attendance units via their web browser and were encouraged to check if they had at least 5 attendance units.
- On December 19, 2013 the second group of 16 students was informed that the distribution of the second set of SCs will take place at the first week of January. Initially this second group of students was informed that they would use the U-Prove technology for evaluating their course. Unfortunately the reference implementation was not applicable to U-Prove smart cards thus we distributed 16 Idemix smart cards instead. The date of distribution was announced at the course's forum as well as in the lecture room.

Figure 5: Lecture Room of Distributed Systems I at the Fall Semester of 2013

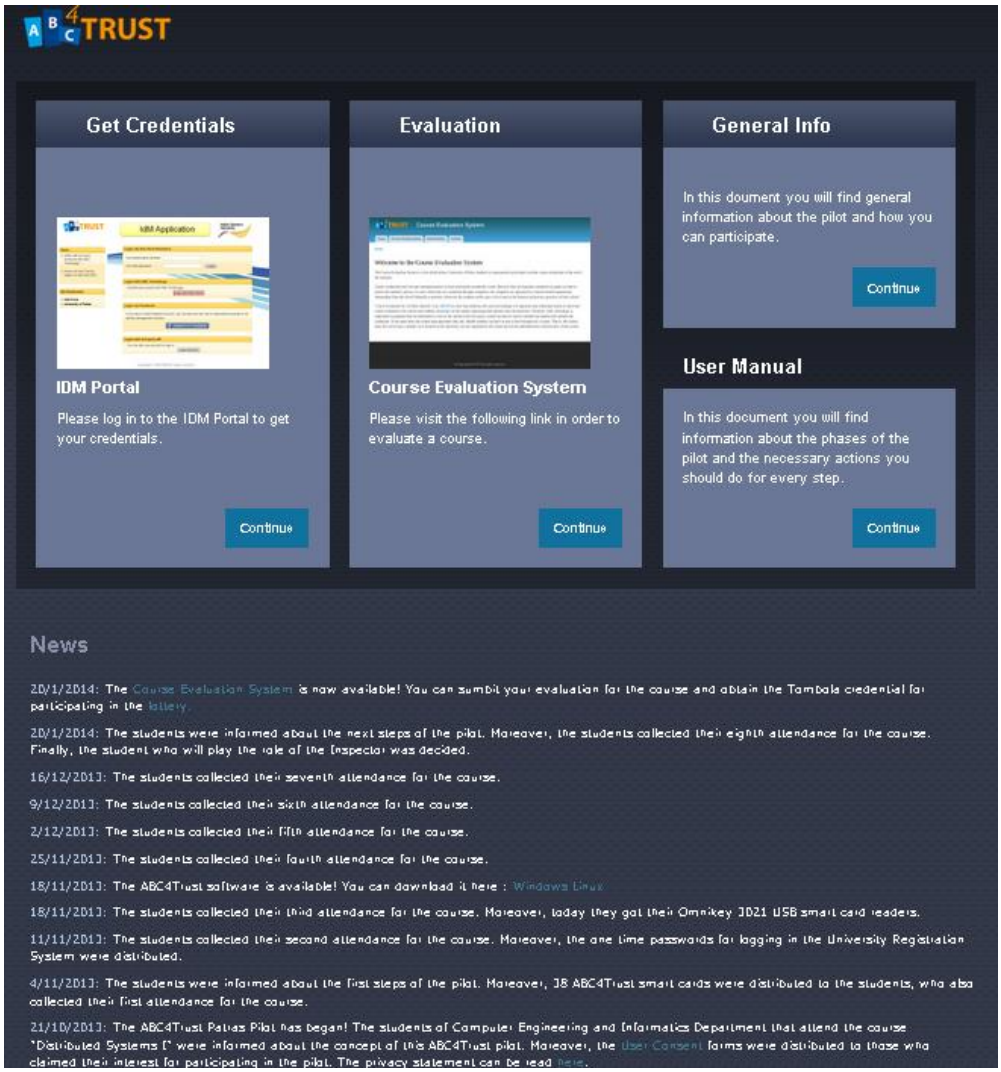


Figure 6: The Patras Portal for the Second Round of Student Pilot

Figure 7: The ABC4Trust Discussion Room at the Course's Forum for the Fall Semester of 2013

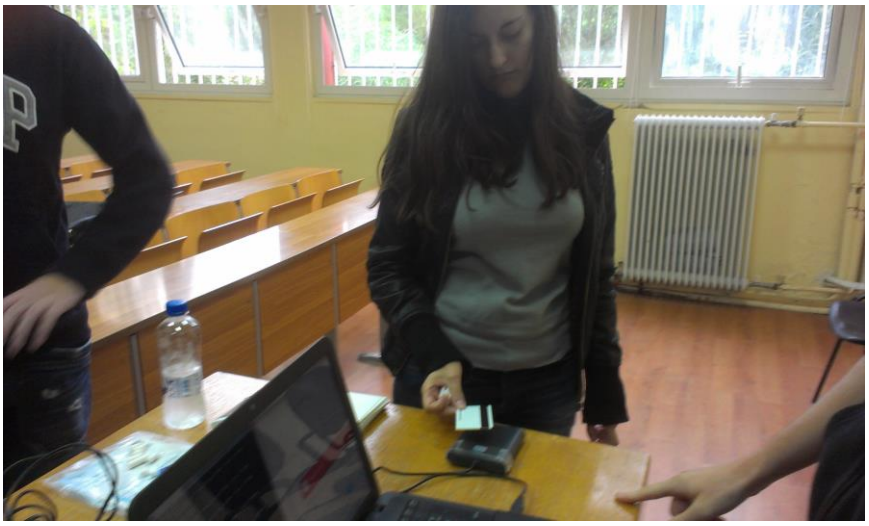


Figure 8: Students Collecting their Attendance Units for the Second Round of Student Pilot

- On January 20, 2014, at the B4 lecture room in B Building, demonstration videos were shown introducing the students to the final steps (course evaluation and tombola game) of the second round of the student pilot. Moreover, the student who will play the role of Inspector was determined. The course evaluation system was launched and made accessible online. All the participating students were informed that they could access the Course Evaluation System until the 26th of January.
- On January 27, 2014, the Tombola System was available. All the 45 participating students were informed that they could join the online lottery game until 22th of February if they had in their possession a tombola credential.
- On February 22, 2014, the tombola got an extension until 26th of February. Moreover, all the 45 participating students were informed that:
  - ✓ The questionnaires would be distributed at the classroom on 26/2/2014.
  - ✓ Alternatively, they could print the questionnaire, fill in their responses, put it in an envelope and put it in Prof. Yannis Stamatiou's (leader of WP7 of the ABC4Trust project) mailbox at the university.
- On February 26 and on March 5, 2014, we distributed the printed questionnaires to the students, at the lecture room. A discussion was organized related to the concepts of Privacy-ABCs, the realization of the pilot and the questionnaire. Finally, the winner of the tombola was announced with the Inspector's help.
- On March 7, 2014, all of the distributed questionnaires were gathered and scanned in digital format for facilitating reference and analysis.

1.2 Structure of the Document

After this brief account of the two pilot rounds, in what follows we will provide and evaluate the findings of our research with respect to the success of the pilot, as well as the ABC4Trust privacy respecting authentication framework.

Overall, the remaining of the document discusses the general feedback from the pilot participants with respect to acceptance and usability of Privacy-ABC technologies, as employed in the pilot system. We first give a general overview of the pilot, and then provide a detailed description of the implemented functionalities for each of the two rounds. Furthermore, this document discusses the degree to which the requirements of the pilot, as set in deliverable D5.1 [SDFBP12], were met. Moreover, it provides a detailed description of the evaluation of the main pilot's components and their services/applications.

Finally, this document includes students' feedback on the User acceptance and participation of the student pilot and the opinions and suggestions of the university's members about the usage of student pilot. We also describe our general and legal considerations for the development and operation of the student pilot and we present our recommendations and guidelines for developing similar and more general applications. For completeness, we discuss the basic steps that the students followed, the actions of the students and the timeline of the two rounds of the pilot. In the appendix, we include all the legal contracts and documents that were prepared for these two rounds. Moreover, in the appendix we also present the content of the distributed questionnaires for the two rounds and the Patras specification document which includes all the technical details of the student pilot.

The chapter organization of this document is as follows:

Chapter 2 presents the student pilot's scenarios for each of the two rounds.

Chapter 3 provides a high-level description of the criteria and requirements that were used in order to evaluate the success of the pilot development and operation. Moreover, it gives a detailed description of the evaluation of the main pilot's components and their services/applications.

Chapter 4 provides a description of the understanding and acceptance of the Privacy-ABC technologies by the participating students.

Chapter 5 provides the legal considerations for the documents used in both rounds of the student pilot.

Chapter 6 presents recommendations for developers and stakeholders and guidelines for developing similar and more general applications.

2 Pilot's Scenarios

As mentioned in the introductory section, the 'Course Rating by Certified Students' pilot had two rounds: the first took place during the Winter semester of 2012/2013 and the second during the fall semester of 2013. In this section, we will describe the pilot's scenarios and the main functionalities that were implemented in each round.

2.1 Functionalities of the First Round

The purpose of the first round of the pilot was to demonstrate some of the basic functionalities of Privacy-ABCs and the reference implementation (mainly credential issuance and verification), as well as to provide early feedback to the reference architecture and reference implementation developers.

According to the chosen scenarios of the first round, the students had to collect credentials that proved, anonymously, that they are students of the University of Patras and that they registered to the course under evaluation. During the semester, they had to attend the course lectures and receive certification (attendance units, one per lecture) about their attendance. Finally, at the end of the semester, they had to anonymously evaluate the course using an online, Privacy-ABCs based, course evaluation system.

The entities that were involved in the first round of the pilot and their corresponding ABC roles were the following:

- University Registration System (ABC Issuer & Verifier).
- Class Attendance System (No ABC role).
- Course Evaluation System (ABC Verifier).
- Students (ABC User).

The students interacted with the University Registration System in order to obtain their credentials. Using these credentials they could prove their studentship and their registration to the course towards the other pilot systems (e. g Course Evaluation System). The Class Attendance System was the system which was operated in the lecture room through which the students obtained attendance units on their SCs. The Course Evaluation System was the system which the students used in order to evaluate, anonymously, the course they had attended. Also, the students had to install an ABC Client Application (User Client Application + GUI, see Figure 9) on their computers in order to be able to interact with the pilot system components.

As soon as the pilot started, we provided the students with an envelope containing a properly initialized smart card and the card's PIN and PUK values. We also gave to each of them a contactless smart card reader and a slip of paper containing a one-time-password for the initial logging in the University Registration System.

The first step for the students was to log in the University Registration System using their matriculation numbers as usernames and their one-time passwords. Then, they were able to register their smart cards so that the University System could link their smart cards with the students' information residing in the IdM database.

After a student had registered her smart card, she was able to obtain the university and course credentials from the University Registration System. The university credential proves the studentship of the participants and includes, as attributes, her first and last names, the name of the university (Patras University), the department name (Computer Engineering & Informatics Department) and finally her matriculation number. The course credential proves that the student is registered to the course under evaluation.

In order to be able to evaluate the course at the end of the semester, the students had to collect a minimum amount of attendance units at the lecture room during the semester. This was accomplished through their interaction with the Class Attendance System. This system, which was operated and supervised by senior personnel of CTI, was located on desk, near the entrance of the lecture room. The students, upon entering the lecture room, had to swipe their smart card in front of the contactless SC reader of the Class Attendance System. This action would trigger the execution of a secure protocol between the smart card and the Class Attendance System at the end of which the attendance unit counter residing in the SC was increased by 1. If the student attempted to obtain, illegally, one more attendance unit by swiping the SC once more, during the lecture (or, in general, during the same day), then the SC software would block the increment operation.

In the end of the semester, the students could access the Course Evaluation System in order to evaluate, anonymously, the course they had attended. The presentation policy of the Course Evaluation System asked from the Users to prove the possession of a course credential as well as present a scope-exclusive pseudonym for the scope "urn:patras:evaluation" bound to the same secret as the course credential. The student's SC permitted the participation in such a proof, only if the attendance unit counter in the card was above the preset attendance threshold.

Finally, the Client Application (ABC User + GUI) installed on the students' computers offered some additional SC related capabilities. Figure 9 shows the ABC4Trust menu of Client Application. More specifically, the Users could browse the credentials stored on their SCs (see Figure 10), change their SC PIN number (see Figure 11) or unlock it using the PUK value (see Figure 12). Moreover, the students could backup and restore the contents of their SCs (see Figure 13 and Figure 14). This functionality was useful in cases of SC loss or damage so that the User would not lose her attendance units.

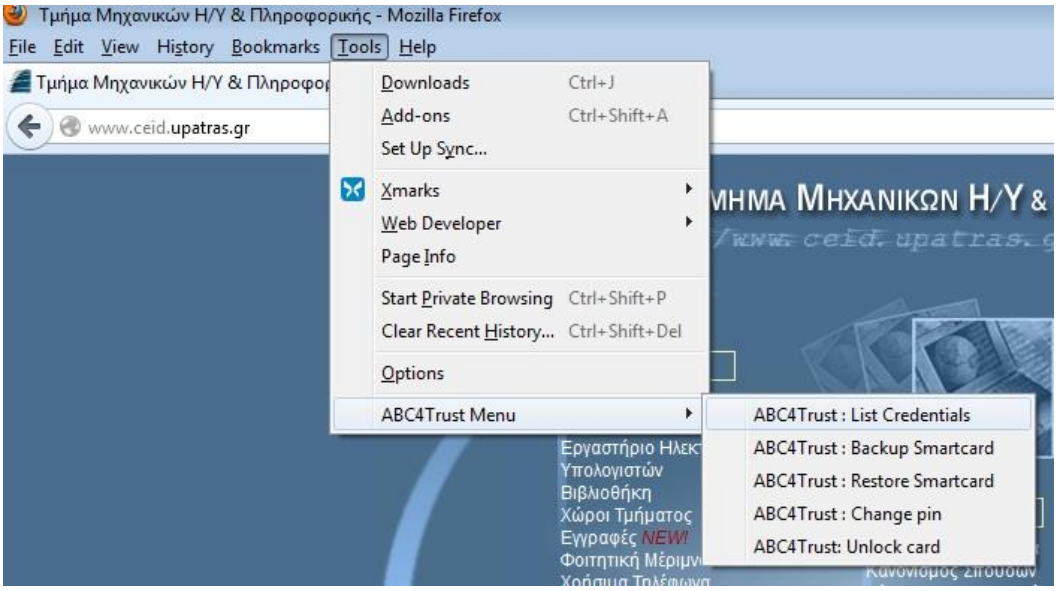


Figure 9: Client Application GUI

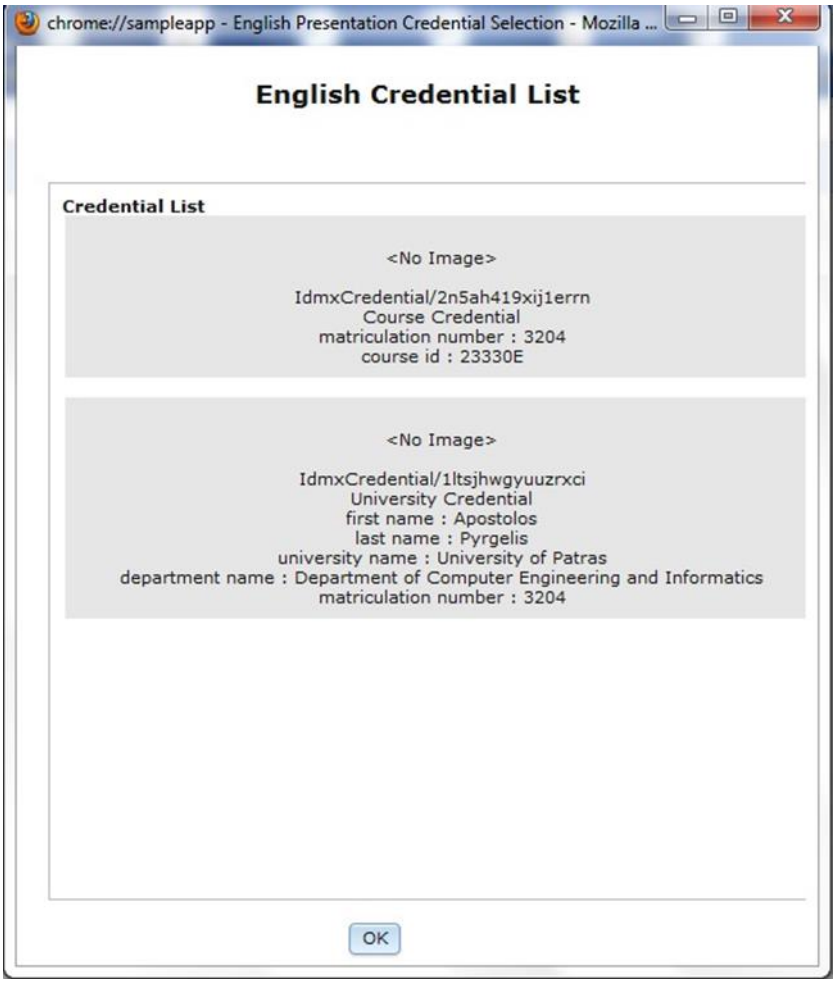
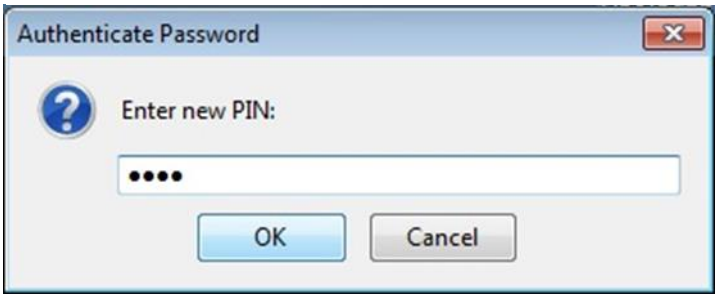
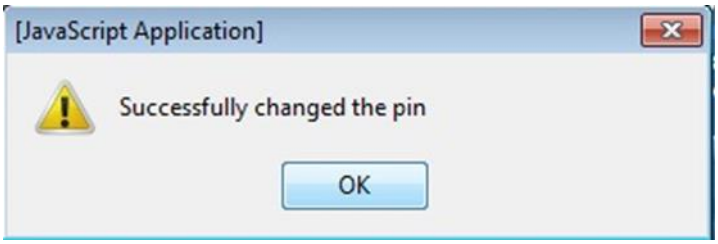


Figure 10: List of Credentials

Step1 : Enter your current PIN



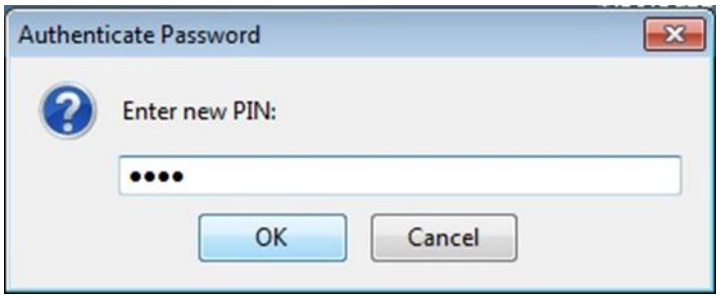
Step2 : Enter your new PIN



Step3 : PIN successfully changed

Figure 11: Client Application Steps for Changing the PIN

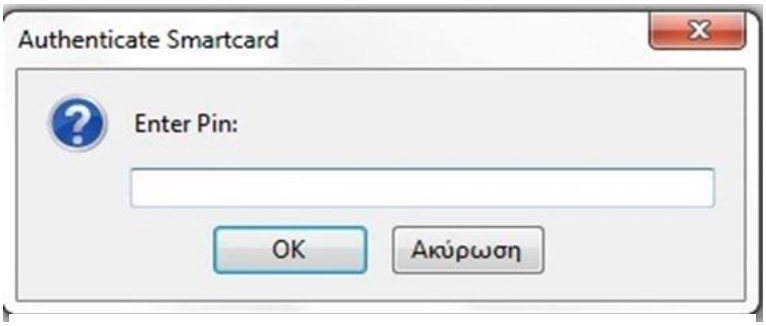
Step1 : Enter your current PUK



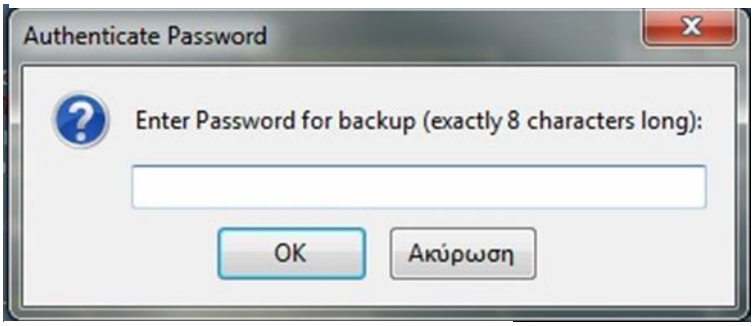
Step2 : Enter your new PIN

Step3 : PIN successfully changed

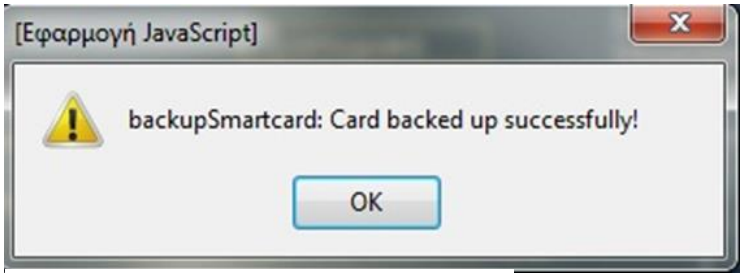
Figure 12: Client Application Steps for Unlocking the SC



Step1 : Smart Card PIN Authentication



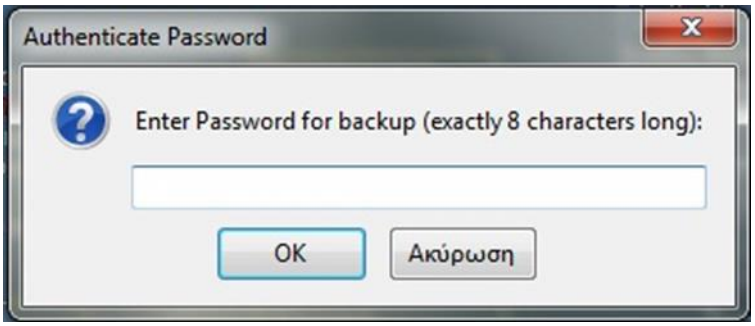
Step2 : Selecting Your Password



Step3 : Successful Back up

Figure 13: Back up SC's data

Step1: Smart Card PIN Authentication



Step2: Enter your password

Step3: Successful Smart Card Restore

Figure 14: Restore the Backed up data

2.2 Functionalities of the Second Round

For the second round of the pilot, we enhanced the scenarios that were used in the first one in order to demonstrate a set of new functionalities and features of the Privacy-ABC technologies. Thus, during the second round a number of additional systems, entities and User steps were introduced to demonstrate and test the advanced features of Privacy-ABCs, including functionalities for revocation, carry-over attributes, and inspection. The detailed description and the technical details of all the functionalities and features of the second round of student pilot is given in the Patras Specification document (see Appendix F).

In brief, the students that participated in the second round had, once again, to collect credentials that proved their studentship and the fact that they were registered for the course that would be evaluated

in the end of the semester. They also had to gather attendance units during the semester at the lecture room. In the end of the semester, they had to evaluate the course they had attended using the Course Evaluation System.

A new scenario that was introduced in the second round, involved the students obtaining an additional credential, called tombola credential, from the Course Evaluation System, after submitting their evaluation. This credential, that proved that they participated in the evaluation, allowed them to access a new (to the second round) system called the "Tombola System". This system is a Privacy-ABCs based Verifier that implements an online lottery which the students can voluntarily enter in order to win a prize e.g., the registration in the 9th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies. This prize acted additionally as an incentive for students to participate in the evaluation of the course.

Apart from the Tombola System, another entity that was introduced in the second round of the pilot was the Revocation Authority. The role of this entity was the revocation (by the administrator) of students' credentials, when necessary. Moreover, in order to protect the students' personal information (mainly to retain anonymity) when accessing the Tombola System, an Inspector entity was also introduced. This trusted entity was necessary in order to decrypt the matriculation number of the winner's presentation token stored in the Tombola System (the rest of the students that took part in the lottery remained anonymous).

In summary, the entities that were involved in this round and their corresponding ABC roles were:

- ✓ University Registration System (ABC Issuer & Verifier).
- ✓ Class Attendance System (No ABC role).
- ✓ Course Evaluation System (ABC Verifier & ABC Issuer).
- ✓ Students (ABC User).
- ✓ Tombola System (ABC Verifier).
- ✓ Revocation Authority (ABC Revocation Authority).
- ✓ Inspector (ABC Inspector).

Figure 15 describes the building blocks of the pilot system in the second round. These blocks and their roles are discussed in Deliverable D5.2 [DCDE12].

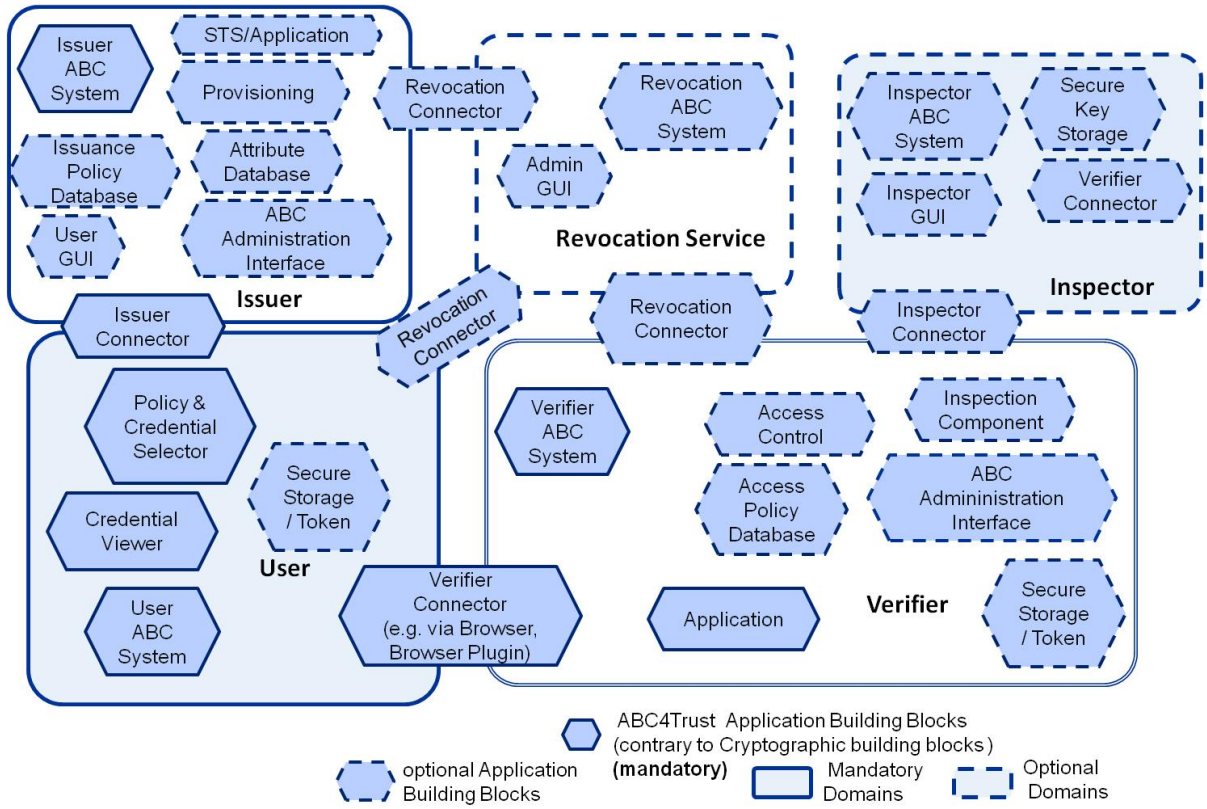


Figure 15: Building Blocks and Domains

In the following, we describe in more detail the features that were introduced in the second round of the pilot.

The first feature that was introduced was the capability of revocation of the university credential. This feature is required in the cases where a student leaves the university or loses her SC. A CTI administrator had the authority to revoke a student's university credential using the University Registration System.

With respect to the Course Evaluation System, we made two basic modifications. First, in order to log in the Course Evaluation System, the student was required to possess a non-revoked university credential and a course credential. She was, additionally, required to present a scope-exclusive pseudonym for the scope "*urn:patras:evaluation"*, bound to the same secret key as the university credential. Moreover, after submitting the course evaluation, the student could engage in an "issuance with carry-over" protocol. During use of this protocol, the student had to prove possession of the scope-exclusive pseudonym that she had previously sent to the Course Evaluation System, upon which her matriculation number was carried over (blindly) from her university credential to a newly issued tombola credential. In this way, the students' anonymity towards the Course Evaluation System was preserved. The Patras specification document presents all the technical details for obtaining this tombola credential (see Appendix F).

After obtaining the tombola credential, the students accessed the Tombola System in order to register for the contest. The Tombola System requested from the students to use their tombola credential and embed their matriculation number verifiably encrypted (with the Inspector's public key), into the presentation token. When the lottery ended, the winning presentation token was given to the Inspector who decrypted the matriculation number out of it, announcing the winner.

Finally, in this round, we provided the students with an updated Client Application which presented to them a friendlier (than the one used in the first round) User interface. As Figures 16 to 20 show, the

new Client Application included new tabs and domains for informing the user about the information which was disclosed, the type of credentials, the pseudonyms' information and credentials' attributes. This module also provided some new functionalities to the students e.g. for deleting credentials, browsing their attendance unit counter stored in their SCs, etc. Additionally, since revocation was active, the backup mechanism was simplified in order to store only the attendance unit information.

Finally, we updated the User Client Application in order to increase the usability of the student pilot. The new Client Application provides all the functionalities that were used in the first round and the additional functionalities of the second round (the figures below show the interface of the new User Application).

More specifically:

- All the participating students installed the new User Client Application on their computer. Every student could then log in to the University Registration System (see Figure 16) in order to get a university or course credential by using the Privacy-ABCs technologies (see Figure 19 and Figure 18).
- All the students that took part in the evaluation can collect their attendance unit at each lecture. Each student could back up her attendance units and restore backed up data on her (new) smart card.
- All the students could view their stored credentials (see Figure 17), could change their PIN of their smart card and could unlock it.
- They were able to prove that they are indeed students of the department offering the course, they are registered to the course under evaluation and they have attended sufficient number of lectures, in order to submit their course evaluation (see Figure 22). The student pilot provides the evaluation of only one course, thus the course identifier (courseID) was not checked in order to increase the efficiency of the student pilot.
- All the students could obtain an additional tombola credential (see Figure 20) from the Course Evaluation System, after submitting their evaluation. This credential allowed them to participate in an online lottery in order to win a prize (see Figure 21).

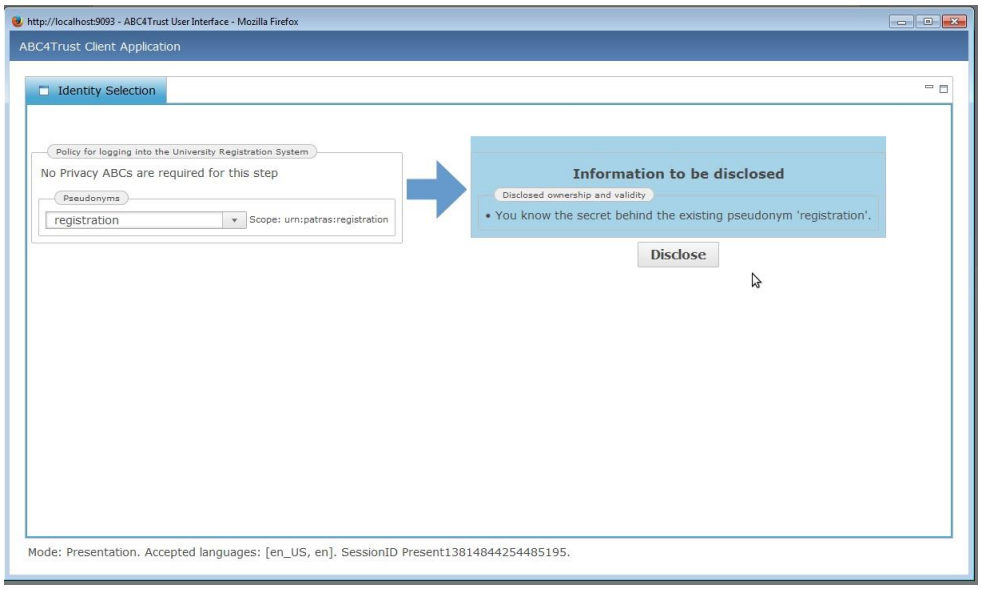


Figure 16: Log in the University Registration System

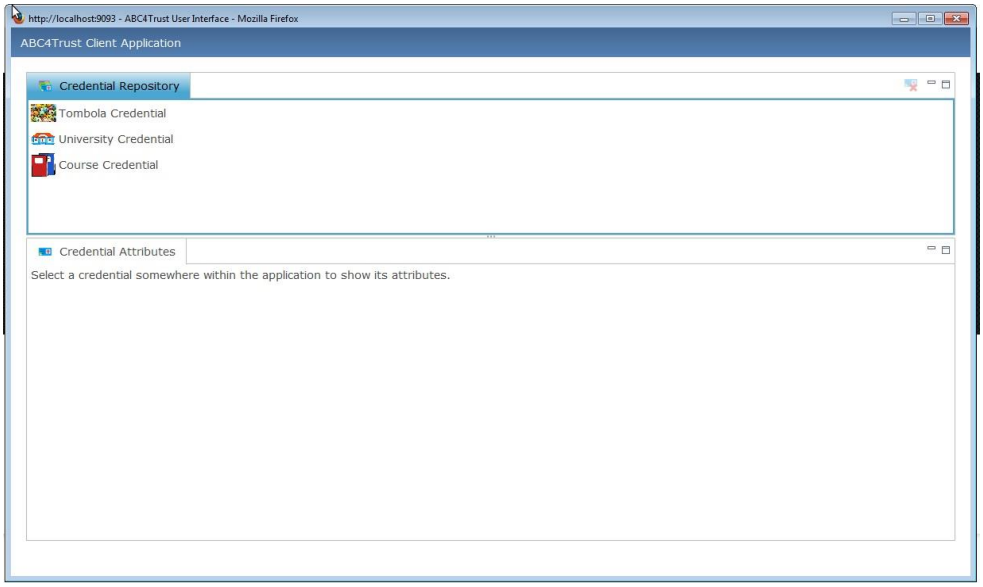


Figure 17: Browse Student's Credentials

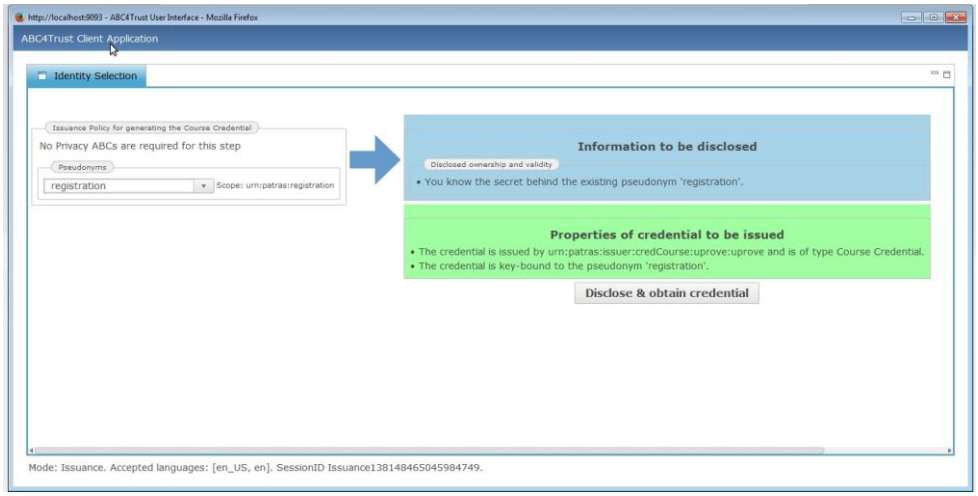


Figure 18: Get a Course Credential

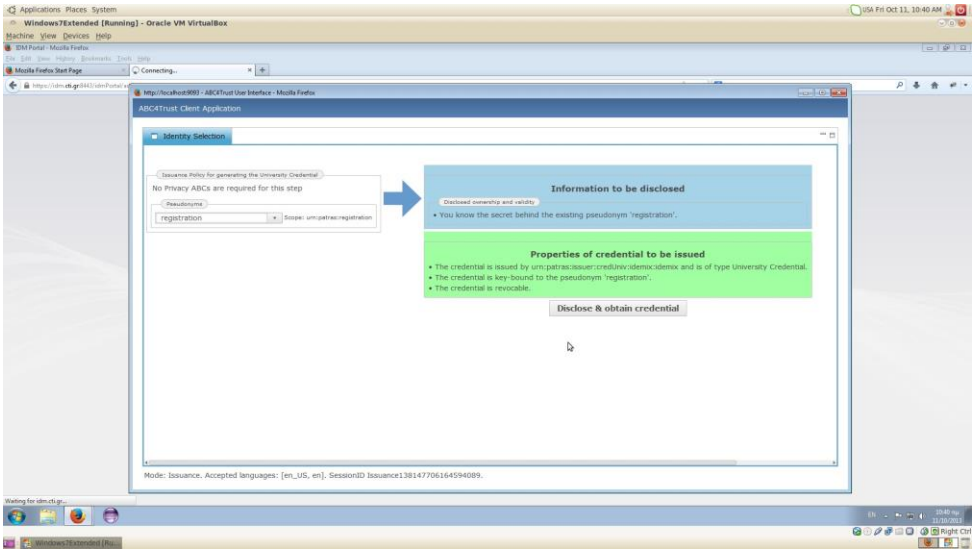


Figure 19: Get a University Credential

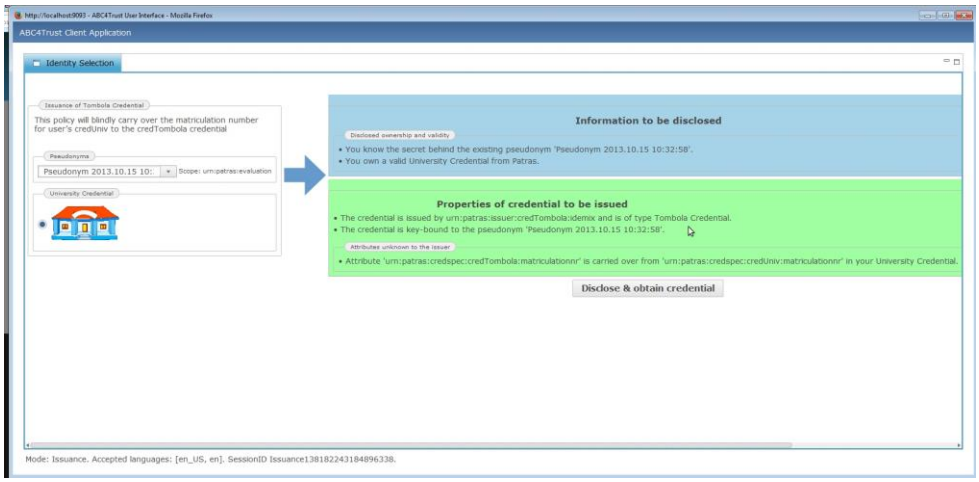


Figure 20: Get a Tombola Credential

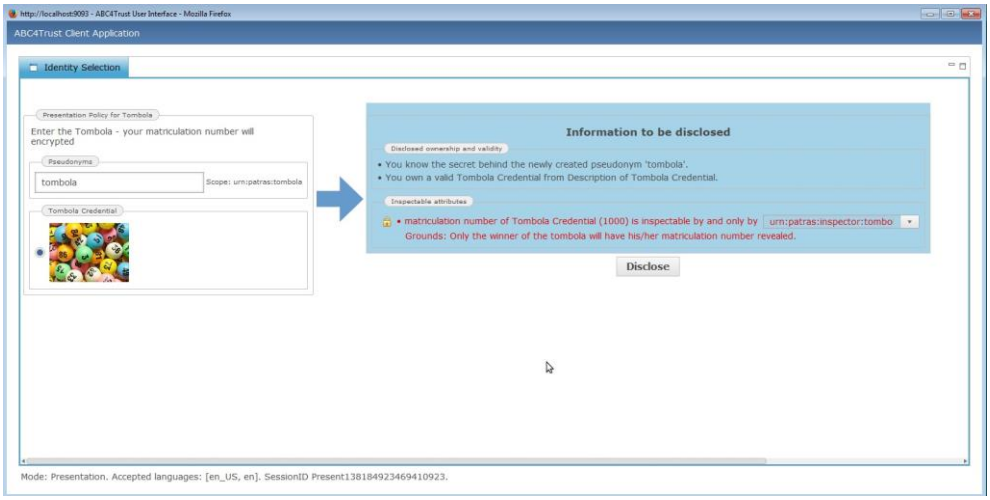


Figure 21: Participate in the Tombola

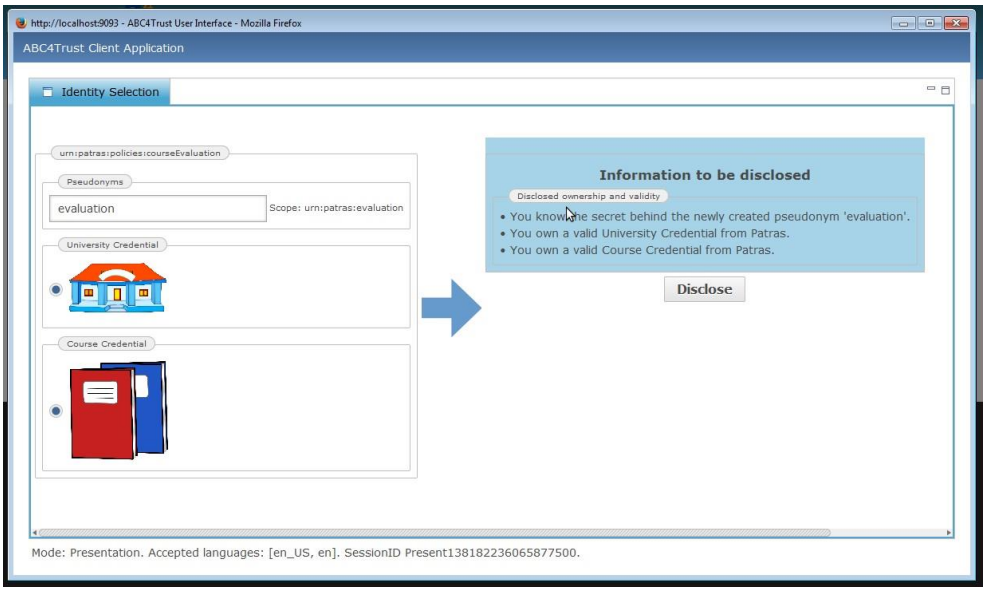


Figure 22: Evaluate the Course

3 Evaluation of Student Pilot's Components

In this section, we evaluate the pilot's basic components from the perspective of the system administrators who were responsible for its operational deployment. More specifically, we provide an evaluation of the network that the system was deployed on, its security, availability and stability. Moreover, we evaluate the applications and the services that the pilot systems offered as well as their response times. Finally, we evaluate the functionality and response time of the smart cards that were used in the pilot.

3.1 Requirements and Fulfillment

Here, we will discuss the degree to which the general pilot requirements were met, as originally presented in D5.1 ([SDFBP12]).

3.1.1 Deployment and Operational Requirements

In this section, we first describe the generic deployment and operational requirements for the success of the first round of the pilot and then the additional requirements of the second round. The requirements for the first round are as follows:

1. Every User should be provided with a contactless smart card reader and a contactless smart card.
2. Privacy-ABCs should be bound to the smart card and/or to the User possessing the SC.
3. The User should not be able to manipulate the presentation tokens or the Privacy-ABCs without violating their integrity.
4. The Privacy-ABCs should be stored on the smart card.
5. Generating an issuance token or a presentation token requires the prior presentation of a valid SC PIN number in order to authenticate the User carrying the card.
6. The User should be able to change the PIN of her smart card.
7. The User should be able to unlock the smart card by entering a valid PUK if a wrong PIN is entered to often (similar to the functionality offered by mobile phone SIM cards).
8. Consent forms should be signed by all participants.
9. A presentation token should be un-linkable to the Privacy-ABCs which were used to generate it, if the User chooses to remain anonymous.
10. During the issuance of Privacy-ABCs, the new credential should be possible to be bound to a User Secret in a way that prevents its valid transfer to another smart card.
11. Both the Verifier and the Issuer should be in position to require the User to insert a pseudonym in her token bound to the User Secret such that the recipients of the token (i.e., the Verifier and Issuer) could be certain that no one else, other than this specific User, could have generated the chosen pseudonym.
12. The User should be in position to generate a token with a specific pseudonym that was used in the past.
13. Both the Verifier and the Issuer require the User to insert a pseudonym in her token which not only is bound to the User Secret, but to a certain scope value (e.g., an URL) as well. In this special case, the Privacy-ABC technologies must force the User to generate the same pseudonym (i.e., scope-exclusive pseudonym) if the scope is the same.
14. The Privacy-ABC technologies must prevent Users from generating tokens from attributes not certified by their own Privacy-ABCs.

15. The Privacy-ABCs technologies must enable all entities to receive and validate tokens, if the tokens are based on attributes of Privacy-ABCs owned by the Users sending the tokens.
16. A replay of the same token should not be permissible by Privacy-ABCs technologies.
17. Log files should be generated by the ABCE and Crypto Engines, which provide information for forensics and liability purposes.
18. The log files should not reveal the values of non-public keys and secrets.
19. The User should be able to generate presentation tokens based on Privacy-ABCs which were issued by different issuers.
20. All the data stored about the Users in the system (including the smart cards) should be deleted after the end of the project.

The resulting generic requirements for the second round include all of the above requirements of the first round of the pilot, as well as the following additional requirements:

1. Revocation of Privacy-ABCs should be enabled.
2. The User should be able to read all the contents of her smart card except the User secret key (this requirement is provided as a built-in feature by the smart card itself). At the second round of the pilot, the User Client Application should allow the User to read her attendance unit counter.
3. During the issuance of Privacy-ABCs, the new credentials can contain attributes from Privacy-ABCs already owned by the User without the Issuer knowing the value of these attributes (i.e. to have carry-over attributes).

3.1.2 Pilot Deployment and Operation Evaluation

Here we describe the specific deployment and operational results that had to be observed in order for the pilot's scenario to be considered a success. In this section we will provide the list of the features that were included and adopted by the student pilot. The realization of the scenarios for each round of course evaluation indicates the following features. Below some general features of the first round of the student pilot are presented.

1. For the On-Site-Testing, 5-10 smart cards with reduced functionality were supplied for the pilot.
2. 54 smart cards with full functionality were supplied. 48 smart cards were equipped with Idemix Privacy-ABC technology and 6 smart cards were equipped with U-Prove Privacy-ABC technology.
3. The User had the possibility of performing a backup and a restore of the attendance data. Restoring attendance data was possible after receiving a new smart card with a new User secret, but it was guaranteed that the attendance data can only be used (for taking part in the course evaluation) by Users who originally received it.
4. The Privacy-ABC technologies supported the generation and verification of the proof.
5. The University Registration System contained a minimal subset of certified attributes for the students.
6. The Class Attendance System was installed on a laptop with sufficient battery power. This offline-system was pre-configured by CTI prior to each lecture and removed from the lecturing room after the lecture.
7. In order to collect attendance units, the students were not requested to enter their PINs.
8. The students got a positive indication (green light signal, tone signal) if they successfully received the attendance unit.
9. The students got a negative indication (red light signal) if there was an error in receiving the attendance units.
10. The User was able to make a backup of her attendance data on trusted hardware
11. The User was able to restore the attendance data on her new smart card

12. A student must only be able take part in the course evaluation process if she possesses the following Privacy-ABCs:
    1. credCourse
    2. sufficient number of attendance units

    The university credential was not revocable thus if a student had in her position a valid course credential she was a student of the department.
13. Privacy-ABC technologies supported the generation and verification of the proof.
14. The User was able to generate a presentation token with a new smart card based on restored attendance data which was issued to her before she lost her old smart card.
15. The User was able to generate a presentation token based on her credCourse if her stored attendance units exceed the threshold value.
16. The User could evaluate the course as many times as she desires during the evaluation period. Privacy-ABC technologies enabled the course evaluation system to take only her last evaluation into account even though she posted her evaluation without revealing her identity.

The second round of the student pilot adopted the most of the above features of the first round of the student pilot and the following additional characteristics:

1. 60 new MultOS smart cards with bigger memory and processing power were distributed to the students. All the 60 smart cards were equipped with both the Privacy-ABC technologies Idemix and U-Prove.
2. When a university credential was issued, a revocation handle was inserted for revocation purposes.
3. The university credential (credUniv) was bound to the smart card secret.
4. A student was able to take part in the course evaluation process if she possesses:
   (1) credCourse
   (2) sufficient number of attendance units
   (3) a non-revoked credUniv
5. A student was able to take part in the tombola if she possesses a valid tombola credential (credTombola)
6. A student was randomly selected to be the Inspector entity. This student received the winner's presentation token and decrypted the matriculation number of the winner and announced the winner of the lottery.
7. All the students that took part in the lottery but did not get the prize, remained anonymous.

3.2 Evaluation of Legal Documents

For both rounds of the pilot in Patras, a series of legal documents had to be drafted. While not all of them are necessary in such detail for each use-case requiring Privacy-ABCs they aimed at providing a high standard of privacy protection for the participants of the pilot. Since the core of the contribution are the legal texts themselves which can be found in the appendixes of this document the following subsections will only elaborate on certain specific issues which had to be considered when drafting the documents. While this section will describe the general considerations for the documents used in both pilots, the subsequent sections will provide the legal considerations for the newly introduced features of the second round.

3.2.1 Legal Documents for both Rounds of the Pilot

The following documents had been drafted for both rounds of the pilot:

- Consent forms for students and lecturers (for more details see Appendix A)

- Information sheet (for more details see Appendix B)
- DPA notification (for more details see Appendix C)
- Processing contract between CTI and NSN (for more details see deliverable D5.3 [EFP14])

3.2.2 Consent forms and Information Sheet for Students and Lecturers

To be able to process the personal data of students and lecturers in accordance with the requirements of the Greek Data Protection Law, the consent of the participants was necessary. According to the Greek national Data Protection Law, consent is

> '*any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognizant signifies his/her informed agreement to personal data relating to her being processed.'*

Therefore, the first prerequisite for a valid consent was that sufficient information was provided to the participants.

> *Such information shall include at least information as to the purpose of processing, the data or data categories being processed, the recipient or categories of recipients of personal data as well as the name, trade name and address of the Controller and his/her representative, if any*.[1]

For further transparency the participants were also informed about where the data would be collected and a high-level outline of the data processing was provided, so they were fully aware of the scope and goal of the pilot. However, to achieve an easy and yet still comprehensive understanding of what was happening with their personal data within this pilot, a multi-layered policy approach was taken. The multi-layered approach meant providing necessary information step-by-step to avoid overwhelming the data subjects with an excessive amount of information at once. Nevertheless, since Privacy-ABCs are still a fairly new technology and not yet well known to the average citizen it seemed necessary to convey complex technical matters and explanations in an easily comprehensive format. However, the target group consisted of students and lecturers from the Computer Technology Institute and therefore a certain level of expertise was assumed. In the end the consent forms themselves were kept short including only the most important and necessary information, yet still comprehensive since they gave links and pointers to further detailed information which was provided continually to the participants of the pilot. Examples would be links to the ABC4Trust website as well as the User Manual. The short consent form was furthermore complemented by a longer information sheet which was handed out together with it. Both documents were revised and adapted to the new features of the second round of the pilot.

Besides being based on sufficient information the consent had to be given freely. This requirement demands that no disadvantages result from not consenting, or that at least the disadvantages are openly communicated to the data subject. Only if data subjects are able to evaluate the benefits and disadvantages of the intended data processing they can make a sensible decision regarding their participation. Therefore, it was stressed in both documents – consent form and information sheet – that not consenting or revoking consent would not have any negative implications on one's participation in the university courses. Furthermore, the online class evaluation of the pilot was complemented by a regular paper-based one for all attendees of the classes regardless of their participation in the trial. Nonetheless, it was explained that a participation in the pilot trial was not possible without consenting to the data processing.

Moreover, a paper-based consent form was preferred to a digital one for several reasons. Firstly, a digital consent form would have required contacting all possible participants electronically before the

[1] See Art. 2 k) of Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data

start of the pilot. Consequently, it would have been necessary to collect the email-addresses of all possible participants. This, however, would have constituted a data-processing in itself and therefore would have presupposed a legal basis. Furthermore, a valid electronic consent would have required that all participants possess a valid digital signature. Eventually a paper-based consent form was preferred for the sake of proof.

Finally, the data of the lecturers had to be considered. While the majority of the data processing concerned the students who were actively involved in the pilot, the pilot also processed personal information of the lecturers to a certain degree. Since certain lectures were evaluated it was necessary to process data in regards to who was teaching which class. Additionally, it was possible that the final class evaluation would also include personal data of the lecturers and therefore their consent had to be obtained as well.

3.2.3 DPA Notification and Processing Contract

In accordance with the Data Protection Directive (Directive 95/46/EC) Article 6 of the Greek Data Protection Law stipulates that the responsible data protection authority has to be notified about the processing of personal data of individuals before the processing commences. Therefore, a written notification was sent to the responsible authority and is attached to this document as appendix. It included information regarding the identity of the controller, the location of the processing hardware, purpose of the processing, the time period until deletion of personal data as well as the identity and involvement of sub processors. Furthermore, the consent forms, information sheet as well as the processing contract between CSI and NSN were attached to the notification.

The aforementioned processing contract between CTI and NSN was needed for establishing a legal foundation for the assistance by NSN. While CTI was the data controller running the ABC4Trust student pilot NSN provided the IdM application and supported the controller with the set-up, administration, debugging, and maintenance of the running IdM system. Consequently, NSN had to be categorized as data processor since it could not be ruled out that NSN would come into contact with personal data of the participants during their troubleshooting tasks. In compliance with Article 10 of the Greek Data Protection Law, it was necessary to bind both parties by a written agreement. However, a detailed explanation of the processing contracts in both pilots can already be found in the sections 2.7.2 and 3.10.2 of the deliverable D 5.3 [EFP14].

3.3 Specific Considerations for the Second Round

The biggest change in the second round of the student pilot was the introduction of inspection as a new feature. Therefore, legal considerations regarding the implementation of this feature will be provided in this section.

3.3.1 Inspection Grounds

Inspection grounds can be defined as the reasons for revealing the real identity of a pseudonymous User by decrypting the inspectable presentation token which includes the identity cryptographically hidden. Consequently, during the inspection the request for inspection and the correlating scenario have to be reviewed in regards to their accordance with the inspection grounds. Different Privacy-ABCs systems will include different inspection grounds, since they have to be adapted to the relevant use-case. However, in most cases a common inspection ground will be a legally justified demand of a third party such as a law enforcement authority. Any additional grounds will be dependent on the purpose of the inspection in the relevant use case. The other ABC4Trust pilot for example, in a school setting in Sweden, included an extensive list of inspection grounds since the school had to ensure the compliance with their policy against discrimination and degrading treatment as well as guarantee the safety of the participating pupils (for further information see section 6.2 of deliverable D6.3 [ESP14]).

The second round of the student pilot on the other hand is an example of a use case with a very limited scope for inspection. The only reason for including the inspection feature was to reveal the identity of a single person – the winner of the tombola. Consequently, the inspection ground for the student pilot was: "Inspection is permitted to identify the winner of a prize and if the prize cannot be awarded to this person for the identification of an alternate winner of the prize."

Besides identifying the winner of the tombola prize, there was no reason imaginable for CTI that would justify an inspection. Even the generic reason of a legally justified demand of a third party such as a law enforcement authority did not appear possible. While it was very unlikely that the evaluation was used as a criminal mean, it was not completely impossible. Nevertheless, even if law enforcement entities would have requested the identification of one or all participants, the inspection of the tombola tokens would have only revealed that a User evaluated the course and used her tombola token for the tombola. Inspection of the tombola token would not have revealed the content of the evaluation sent by a User. On top of that the scope-exclusive pseudonyms of the evaluation systems and the tombola system were not linkable and the course evaluation itself system did never obtain the matriculation number or any other linkable information from the students. Furthermore, the course evaluation system did not store any information about the students IP-addresses. Moreover, in the case that only a very limited number of students would have evaluated the course at all, the whole set of collected evaluation data would have been deleted from the course evaluation system. Consequently, the inspection itself would not have helped to identify a User beyond the inspection ground and seemed therefore useless for any official investigation.

However, since the inspection feature allows to identify the User and inspectable presentation tokens restrict Users to pseudonymous interactions, instead of anonymous ones, the feature itself interferes with the right to privacy. Consequently, providing information to the User is of upmost importance. This information should include a detailed description of the inspection grounds, the procedure of inspection and whether additional parties will be involved as a safeguard against abuse of inspection. Nevertheless, the exact scope and how the information is provided to the Users, is dependent on the inspection grounds, because they determine how intensely the right to privacy is constrained.

The second round of the student pilot was a less complex case of inspection with a very limited inspection ground. Furthermore, the participation in the tombola was voluntarily and the utilization of the inspectable presentation token provided the Users only with an additional benefit – the chance of winning the tombola. Not using the token, however, did not result in any disadvantage, since the participation in the test pilot was still possible. Therefore it was sufficient to stipulate the sole reason for inspection in the consent form.

3.3.2 Description of Inspection Process

As mentioned before, it is necessary to describe the process of the inspection to the Users in addition to informing them about the specific inspection grounds. In the Patras case it made sense to indicate which system is having which type of information and how they interact with each other. In detail, there were three phases which had to be elaborated on - starting at obtaining the information through the Course Evaluation System and ending with the inspection for the tombola. While these phases will be explained here, all previous steps of the pilot such as initialization of cards or obtaining credentials etc., will not be discussed in this section:

1. *Evaluation phase*: Students use the university credential to verify their status as an enrolled student towards the system and provide the evaluation data in form of answers to the question provided about the quality of the lecture. The evaluation data is stored on the Course Evaluation System. To ensure that participants may resume the evaluation or change their replies until the end of the evaluation period the User can re-authenticate on basis of a scope exclusive pseudonym reliably proving that the same User interacts with the system. The scope for this purpose is "urn:patras:evaluation". A check for the minimum participation is done. If the size of the sample does not reach the size of the previously defined minimum anonymity

set, it was foreseen that the evaluation data will be deleted. In this case, this particular lecture cannot be evaluated due to lack of data material. After finishing the evaluation, the Users had the possibility to obtain a tombola credential for a voluntary participation in the tombola.

2. *Join tombola:* The User joins the tombola by providing proof of participation in the evaluation with her tombola credential. In addition, the inspectable part of the token provided containing the matriculation number is produced on basis of the university credential. To ensure that a User may only join the tombola once, a scope exclusive pseudonym is obtained allowing the re-identification of a User accessing the system more than once. The scope for this purpose is "urn:patras:tombola". Since the tombola credential is stored on the smart card and cannot be obtained after the course evaluation period is over, it may be possible to lose the smart card after the end of the evaluation period and before using the tombola credential. In this case, it is not possible to regain the lost tombola credential since it is no longer issued by the course evaluation system. This risk was labeled as acceptable within the limited scope of this pilot.

3. *Tombola execution:*
    a. Once the timeline for joining the tombola is closed, the list of valid tokens is produced. Under supervision of one or more students, the winner is drawn. This may happen e.g. on basis of a numbered list with the hash-values of the tokens where a random number decides about the winner. The presentation policy of the Tombola System demands from the User to prove the possession of a scope-exclusive pseudonym for the scope "urn:patras:tombola". The Tombola System checks if the pseudonym has already been registered and if so the registration process is terminated.
    b. Inspection: The winning presentation token is submitted to the designated Inspector. For the second round of the pilot, a randomly selected student from within the course takes this role, decrypts the content of the token and proclaims the winner. In case the winner does not claim the prize within the previously defined timeframe, step 3 is repeated. Even students who are no longer a member of the university are eligible to win the price since the prize is not bound to still being a student at the university, but taking part in the course evaluation during the pilot runtime.
    c. Deletion of data: Once the prize has been awarded, the tokens submitted for the tombola are deleted as the sole purpose of the processing has been achieved.

The process can be depicted in a flow diagram as shown in Figure 23 below.

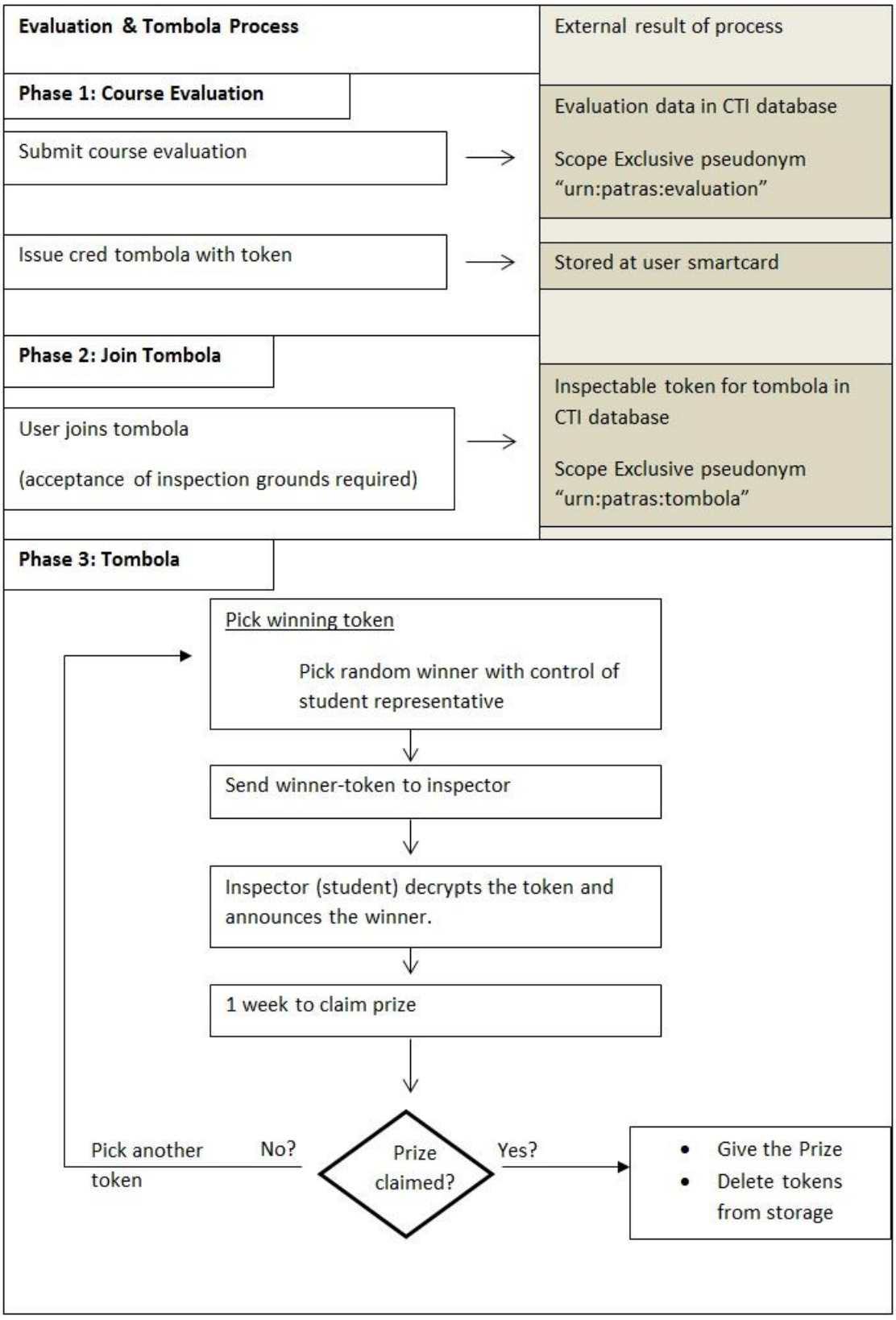


Figure 23: Flow of the Evaluation and Tombola Processes

3.3.3 Summary of legal considerations for inspection

In summary of the legal considerations for inspection, the following aspects may be noted:

- Documentation and description of the inspection processes is a prerequisite for a valid informed consent and necessary to comply with the privacy protection goal of transparency. In particular, this advanced feature should be described thoroughly to enable Users to fully understand what happens with their personal data. Furthermore, since Privacy-ABCs are more privacy protecting than other possibilities, even when they include inspection, comprehending the system might lead to the situation that Users gain additional trust in the data controller once they have realized that the data controller takes measures to process as little personal data as possible.
- Where unlinkability is desirable between systems, such as between the Course Evaluation System and the Tombola System here, the scope exclusive pseudonyms must be different. Additionally to avoid even linkability by timestamps in the student pilot, participation in the tombola was not available for some time after the course evaluation system was closed.
- Likewise inspection tokens must be unlinkable even if the same content is encrypted inside.

3.4 Evaluation of Student Pilot's Network

3.4.1 First Round

As described in more detail in D7.2 ([NHSPSPD]), the servers required for the pilot systems (University Registration System, Course Evaluation System) were hosted in CTI's internal network, which is reachable through GRNET. GRNET provides high quality services of national and international interconnection and capacity in the Greek research, academic and educational community, covering their ever-increasing requirements for high level services and Internet applications. So, students with fast internet connections could reach the pilot systems with minimum delay. Moreover, special security configurations (for details see next subsection) were in place, in order to protect the servers from various attacks. Finally, during the first round of the pilot no power failures that would take down the servers occurred. As a result, the students that participated in the pilot could access the web applications at any time without facing any problems or difficulties.

3.4.2 Second Round

Similarly to the first round of the student pilot, the systems required for the second round (University Registration System, Revocation Authority, Course Evaluation System and Tombola System) were hosted on servers located on CTI's premises and reachable through CTI's internal network. During the operation of the second round of the student pilot, one minor issue regarding the connectivity to the pilot systems came up. This issue was expected as it was related to maintenance tasks in the CTI's internal network. More specifically, it was announced by CTI's network operators that on Saturday 22/2/2014 the Internet connectivity of our systems would be blocked between 8 am until 13 pm. The pilot administrators had informed earlier the students about this issue. Moreover, since the tombola deadline was set for that Saturday the administrators decided to extend the lottery until Wednesday 26/2/2014 for those students that would miss the deadline due to the connectivity issue.

3.5 Evaluation of Student Pilot's System Security

3.5.1 First Round

As described in the network architecture figure (for more details see D7.2 [NHSPSPD]), the network's security was ensured by the existence of a pair of firewalls (Cisco Pix-535). The firewalls were connected between the border router (Cisco 7300 series) and CTI's internal network, controlling incoming and outgoing traffic, thus ensuring network security and protection against malicious attacks. Firewalls can block source IP addresses in the case of Denial of Service (DoS) attacks as well as traffic to non-authorized addresses in CTI's internal network. At the border router we implemented some generic access lists in order to increase the level of security and confront some types of malicious attacks. During the deployment of the first student pilot we did not notice any suspicious traffic and no DDoS/DoS attacks were launched.

Moreover, all the communications between the Users and the pilot system were over a secure and authenticated channel (using HTTPS). As a result, the communication between the Users and the pilot systems could not be intercepted by unauthorized parties.

Finally, students and lecturers had their own local accounts for accessing the pilot systems through the Internet whereas pilot administrators could establish VPN connections and communicate with the pilot systems via SSH or LDAP. No unauthorized access to the pilot systems was observed during the operation of the pilot.

3.5.2 Second Round

Since at the first round of the student pilot was not faced any security issues, the same security measures were kept in place for the second round. The firewall rules that were set by the network operators prevented any types of malicious attacks. The communication with the pilot systems (even the new ones we introduced, i.e., Revocation Authority and Tombola System) were over secure and authenticated channels, so that it could not be intercepted by unauthorized parties. As a result, the pilot administrators did not have to deal with any system attacks and no unauthorized access to the pilot systems was observed during the second round of the student pilot.

3.6 Evaluation of Student Pilot's Availability

3.6.1 First Round

As mentioned above, during the first pilot round there were no connectivity problems with the pilot systems and the students could access them through HTTP/HTTPS connections at any time. However, some availability issues were reported by the students and they concerned the ABC4Trust installer, the smart cards, the smart card reader drivers and the multiple Users' concurrent access of the pilot systems. In more detail, the availability issues were the following:

- Students who were using the 64-bit version of Windows 7 had some problems with the ABC4Trust User Client Application installer. More specifically, the installer when executed could not install successfully the browser plugin. As a result, the students could not interact with the pilot systems. The solution to this issue was to provide a new updated version of the installer to the students.
- Another issue regarding the ABC4Trust installer was that the User Client Application could not be initialized properly on some Users' PCs. Having this issue, the student could not interact with the pilot systems. However, this problem's cause was a broken installation of Java on the User's PC. The solution to this issue was to uninstall Java and re-install the ABC4Trust installer which would install Java successfully.

- The smart card reader (Omnikey 3021 USB) drivers were not installed properly on some User PCs when using the Windows Update Manager. Thus, the User-Service running on the User's PC could not communicate with the student's smart card and no interaction with the pilot systems could take place. The pilot administrators advised the students who had this problem to download and install manually the smart card reader drivers from the Omnikey website and this availability issue was resolved.
- Some students tried to obtain their credentials multiple times from the University Registration System and their smart cards ran out of memory. As a result, the smart card could not function properly and the students could no longer interact with the pilot systems. The solution to this availability issue was for the students to contact a pilot administrator who would re-initialize their smart cards and advise them to re-obtain their credentials but only once.
- When students tried to simultaneously access a pilot system (e.g., log in to the Course Evaluation System at the same time) the system's ABCE layer could not handle all the requests. As a result, some students were not allowed to log in at that point. However, if they tried a few seconds later they could log in successfully. This issue was expected since the reference implementation of the ABCE was not designed to be "thread-safe" at that point in time.

All the above availability issues were resolved successfully by the pilot administrators with the help of the ABC4Trust consortium. Moreover, some of these issues (smart card, concurrent User access of the ABCE layer) were taken into account in order to be mitigated in the project's reference implementation and be successfully deployed on the second round of the pilot.

3.6.2 Second Round

Apart from the connectivity problem that was mentioned in Section 3.4.2, another availability issue came up during the operation of the second round of the student pilot. This issue appeared on the first weekend of February (1st and 2nd day of February 2014). It was unexpected and it was related to power failures at the CTI premises. These failures came up due to bad weather conditions that affected CTI's power supply infrastructure. As a result, the pilot systems were down for that specific weekend. The students were immediately informed about this issue and they were provided updated information as soon as the issue was resolved and the systems were up again. Some other availability issues that were reported by the pilot students are the following:

- A few students contacted the pilot administrators claiming that they could not log in at the University Registration System using their matriculation number and the One Time Password that was provided to them. The admins by checking the server log files found out that the User side was presenting an invalid cookie when trying to log in. Thus, they advised the students to clear their browser cookies and cache and re-try to log in. This issue would be resolved successfully.
- Some students who had installed properly the User Client Application on their PCs, had some trouble during their interaction with the pilot systems (e.g., when trying to register their smart card at the IdM Portal). This issue was related to the fact that the smart card reader drivers (Omnikey 3021 USB) were not installed correctly on their PCs and as a result the User Client Application could not communicate with the smart card. As soon as they were advised by the pilot administrators to download and install manually the smart card reader drivers from the Omnikey website, this issue would be resolved.
- It was mentioned by some students that they could not unlock their smart card after accidentally locking it (i.e., by inserting the wrong PIN 3 times in a row). When they launched the "Unlock Your Smart Card" functionality from the browser plugin and the PUK value was

inserted, the operation would not complete successfully in cases where the PUK value was shorter than 8 digits (such a case is possible to happen when initializing the smart card). That was because the User Client Application was programmed to handle only PUK values 8 digits long. In order to resolve this issue the administrators provided the students with a script that when executed would ask from the Users the smart card PUK value and would allow them to unlock their smart card successfully.

- As a result of the previous availability issue, some students who had their smart cards in locked mode (and could not unlock it due to their PUK value being shorter than 8 digits) could not obtain attendance units during the course lectures. That was expected since when the smart card is in locked mode, it cannot accept any commands (APDUs) unless it gets unlocked first. This issue was resolved after the student would execute the script that was provided by the pilot admins for unlocking the smart card (no matter what the PUK length was).
- Similarly to the first round, some students obtained their university and course credentials multiple times from the University Registration System. As a result, (although the MULTOS smart card had bigger memory than the Basic card used in the first round) the smart card did not have sufficient space to store the tombola credential when obtained from the Course Evaluation System. The students were advised by the administrators to delete the unnecessary credentials using the Credential Manager functionality of the User Application. As soon as the students would delete the redundant credentials from their smart card, the issuance protocol would complete successfully and the tombola credential would be stored on the card. We here note that even if the smart card could not fit a credential in its storage space, it would not break down during the issuance protocol as in the first round of the pilot (i.e. the out of memory exception) and it could be used normally for future operations.

Having the experience from the first round of the student pilot, the administrators could deal easily with the availability issues that came up during the second round. As one can notice, the major issues that were discovered during the first pilot (concurrent processing at the ABCE layer, smart card memory exception) did not affect the operation of this round.

3.7 Evaluation of Student Pilot's Services/Applications

3.7.1 First Round

The University Registration System was the system that the students interacted with in order to collect their credentials. This system contained a database that stored the students' attributes. The database was administered by pilot administrators using an LDAP administration tool. The applications offered by the University Registration System were the IdM Portal, the IdM Application and the IdM Smart Card Registrar. The IdM Portal provided a GUI to the students for browsing the attributes that are stored about them, registering their smart card and obtaining their Privacy-ABCs. The IdM Application represented the backend of the IdM and was used by the IdM Portal in order to authenticate the Users. Finally, the IdM Smart Card Registrar was an application accessed only by the pilot administrators in order to register the smart cards' scope exclusive pseudonyms to the IdM database. All the University Registration System applications were working properly and the administrators did not face any issues with them during the pilot.

Moreover, as the University Registration System was an ABC Issuer as well as an ABC Verifier, it contained an ABC layer that offered the issuance/verification services. These services could be accessed by the students through HTTPS connections. As mentioned in the availability sub-section, some issues were reported when students tried to access simultaneously some of these services e.g., when 2 or more students tried to log in to the University Registration System via Privacy-ABC tokens at the same time. However, this issue was expected since the ABCE layer at that point in time was not designed to handle multiple simultaneous connections.

As soon as the students had collected sufficient attendance units for the course lectures they could log in to the Course Evaluation System and fill in the questionnaire regarding the course. The Course Evaluation System had a database for storing the students' submissions and application related data. Moreover, it consisted of a web application that presented the necessary GUIs to the students for logging-in and submitting their evaluation. There were no problems reported regarding the Course Evaluation Application. Finally, as the Course Evaluation System was an ABC-Verifier, it consisted of an ABCE layer that provided the verification service. This service could be accessed by the students through HTTPS connections. Some problems were reported by students who accidentally tried to log-in to the Course Evaluation System at the same time, but that was expected as explained previously. When they tried it again later on, they logged in successfully and completed their evaluations.

In order to setup the User-side tools, we provided the students with an appropriate installer. Basic requirements for this software were the Java Runtime Environment and the .NET framework. If these were not available on the User's PC, they were downloaded and installed by the installer. Moreover, when executing this installer, the ABC4Trust User Client Application was up and running at the User's PC and a plug-in was installed in her browser. An issue that was reported by some students that were using the 64-bit version of Windows 7 was that after executing the installer the browser plug-in was not installed in their browsers. After that, we provided a new version of the installer that solved this issue successfully. Additionally, some students had a broken Java installation on their PCs and as a result the ABC4Trust User Client Application could not be initialized properly. We advised these students to un-install Java and re-install the ABC4Trust installer. After this step, their environment was setup appropriately in order to interact with the pilot systems.

3.7.2 Second Round

Similar to the first round, the University Registration System was the system that the students would interact with in order to register their smart cards and obtain their university and course credentials. Apart from some minor usability/availability issues (see Section 3.6.2), the students did not face any problems when using this system. The Course Evaluation System was now playing the ABC role of Verifier and Issuer. It allowed only certified students, i.e., students who possessed a university and a course credential and also had sufficient attendance units on their smart card, to log in and submit their evaluation for the course. After submitting an evaluation for the course, a student was able to obtain a new credential called tombola credential. This credential would allow her to join an online lottery. Some students faced a problem when trying to obtain the tombola credential but it was related to their smart card not having enough storage space. As soon as they would delete their redundant credentials, they would be able to obtain the tombola credential successfully. The Class Attendance System was the same application as in the first round and it was working properly during the course lectures. One minor issue that we observed was that some students could not obtain their attendance when their smart card was in locked mode. This issue was expected (the card cannot accept any commands when it is in locked mode) and the student had to unlock her smart card using the User Client Application and the PUK value in order to obtain her attendance unit.

For the second round of the student pilot, we introduced some new applications. The Tombola System was playing the ABC role of Verifier and allowed only students who had obtained the tombola credential to register for the online lottery. The presentation policy of the Tombola System demanded from the students to prove possession of a tombola credential and encrypt the matriculation number with the Inspector's public key. Thus, the presentation tokens that were registered at the Tombola System database contained the student's matriculation number encrypted with the Inspector's public key. The students who had evaluated the course and obtained the tombola credential could register for the lottery without problems. After the lottery phase ended, the pilot administrators provided the Inspector with the presentation token that was selected as the winner from the system. The Inspector executed the Inspector Application along with her smart card (which contained the Inspector's secret key) and decrypted the matriculation number from that token. The winner was then announced to the rest of the pilot participants. No issues came up when using the Inspector Application. Additionally,

for this round we introduced the Revocation Authority. Using the IdM Admin GUI (a service which was in communication with the Revocation Authority) the pilot administrators could revoke a university credential when required e.g., when a student smart card was lost or when a student would graduate. The Revocation Authority services should be online 24/7 since other applications (e.g., Course Evaluation System, User Application) require it in order to collect the latest revocation information. During the pilot, the administrators did not come up with any such problems regarding the Revocation Authority.

Finally, in order to set up the User side the pilot administrators provided the students with an installer. When executed, the installer would install the required software (i.e., Java), would download the pilot resources (system parameters, issuer resources, inspector public key, revocation authority parameters etc.) from the bundle that was uploaded on the ABC4Trust SFTP server. Moreover, the installer would install the Firefox browser plugin and would initialize the ABC4Trust User Client Application on the User's PC. There were no issues reported by the students regarding the operation of the ABC4Trust installer.

3.8 Evaluation of Student Pilot's Response Time

3.8.1 First Round

When evaluating an online system that Users interact with, an important factor to deal with is the response time. During the first round of the pilot, we measured approximately the timings for the pilot's basic operations.

The pilot administrators prior to pilot deployment had to perform some actions like loading the smart cards with the ABC4Trust Application (20 seconds), initializing the students' smart cards with the appropriate parameters (approximately 10 seconds per smart card) and registering the smart cards' scope-exclusive pseudonyms at the IdM database through the Smart Card Registrar (6 seconds).

As soon as the students received their smart cards, they had to interact with the University Registration System. Their first action was to register their smart card which lasted approximately 6 seconds. After that, they could engage in issuance protocol and obtain their university credential (19 seconds) and the course credential (18 seconds).

Obtaining the attendance units when interacting with the Class Attendance System during a course lecture was measured at an average 1.5 seconds (no ABCE protocol involved). When logging in at the Course Evaluation System at the end of the semester, the students engaged in a verification protocol whose completion required approximately 14 seconds on average.

We note here that these timings include possible network delays, processing delays at the User side (User Client Application and smart card) as well as the processing time on the server side. When considering the heavy cryptographic operations that are executed during issuance and verification, the timings provided are acceptable.

Finally, the smart card related operations provided by the User Client Application were sufficiently fast as well. Browsing the credentials stored on a student's smart card took approximately 2 seconds, changing the smart card's PIN or unlocking it with PUK value needed 1 second. Moreover, keeping a backup of the smart card contents required 3 seconds and restoring the backed up content on a new smart card took 2 seconds.

3.8.2 Second Round

In the second round of the student pilot we deployed the newly developed Reference Implementation, which was based on the new cryptographic architecture implemented by WP4. With the new crypto architecture in place, we could now have interoperability between Idemix and U-Prove (no distinction

between Idemix and U-Prove smart cards) and we could also use the 1024 bit length for the system security. Moreover, we used a different smart card (MULTOS smart card) than the one used in the first round (Zeit Basic Card). For these reasons, the response times of the pilot systems were different than those of the first round of the pilot.

The first administrator's task was to load the smart card application (i.e. the pre-compiled ALU file) on a MULTOS smart card which required approximately 35 seconds. The smart card initialization procedure (i.e. set up a smart card with PIN, PUK, system resources and scope-exclusive pseudonym) needed around 7 seconds. Finally, registering the smart card pseudonym at the IdM database using the Smart Card Registrar required around 5 seconds.

As soon as the smart card was distributed to a student, she would have to register it through the IdM Portal. This operation would take around 5 seconds. The next actions would be to obtain her university credential (15 seconds) and her course credential (9 seconds) from the University Registration System. Obtaining the university credential required more time than obtaining the course credential since it included more attributes. Moreover, the Issuer had to contact the Revocation Authority in order to obtain a revocation handle (please note that only credUniv was revocable).

In order to obtain the attendance unit when interacting with the Class Attendance System during a course lecture the student would require 1.5 seconds. Next, the student could log-in to the Course Evaluation System by presenting her valid (i.e., not revoked) credUniv and her credCourse. This presentation protocol would require around 20 seconds in order to complete (the Course Evaluation System had to contact the Revocation Authority in order to obtain the latest revocation information which required approximately 4 seconds). As soon as the student would submit her evaluation for the course she could get issued the tombola credential for participating in the online lottery. This issuance protocol includes a carry-over attribute (matriculation number from credUniv is carried over to credTombola) and requires approximately 17 seconds to complete. Then presenting the tombola credential to the Tombola System (the matriculation number is encrypted with the Inspector's public key) requires around 11 seconds.

The above time measurements include possible network delays, processing time at the User side as well as the server side. It is not meaningful to compare these timings with those of the first round since the scenario is quite different (it has new features and functionalities, lower key size, introduction of Revocation Authority and Inspection). However, one could observe that the overall system performs quite well considering the heavy cryptographic operations that are computed on the smart card.

Regarding the Inspection process, the Inspector used the Inspector Application along with her smart card in order to reveal the matriculation number out of a presentation token. This operation required around 5 seconds. Moreover, regarding revocation a pilot administrator required 1 second in order to revoke a student credential via the IdM Admin GUI.

Finally, the operations provided by the User Client Application regarding the User smart card are quite efficient. A student can browse her credentials that are stored on her smart card in 7 seconds and can be informed about how many lectures she has attended in 1 second. Changing the smart card PIN value (using the PUK value) requires around 1 second, keeping a smart card backup and then restoring it needs around 1 second.

3.9 Evaluation of Smart Cards and Smart Card Readers

3.9.1 First Round

Every time the students attended a course lecture, they interacted with the Class Attendance System in order to obtain one more attendance units on their smart cards. The Class Attendance System was hosted on a laptop with an NFC smart card reader attached to its USB port (Figure 24). The Class Attendance Application was running on the laptop setup by a teaching assistant prior to each lecture.

As soon as a student swiped her smart card near the NFC smart card reader (see Figure 24), a protocol was executed between the card and the Class Attendance Application. During this protocol, the smart card was ensured that it was communicating with the valid Class Attendance System and an attendance counter stored on its memory was increased by one (in case of a new lecture). The Class Attendance Application was working properly and the protocol execution with the smart card was running in approximately 1.5 seconds. This response time was fast enough so that the students would not queue up at the entrance in order to collect their attendance units, affecting the start time of the lecture.

During the first pilot round, we distributed to the students properly initialized SCs loaded with the ABC4Trust Smart Card application. Using the smart cards along with the User Client Application installed on their PCs, the students could interact with the pilot systems and participate in Privacy credential issuance and in token presentation. The response time of the smart cards when participating in such protocols was a little slow e.g. they needed 8 seconds to complete a zero-knowledge proof protocol. However, that delay is reasonable considering the heavy cryptographic computations required. Moreover, the smart card application developer did not have access to low level APIs for big number arithmetic.

As the pilot had already started, it turned out that the smart card's memory was not sufficient to store more than 4 credentials. Thus, when some students tried to obtain their credentials from the University Registration System multiple times the smart card return an "Out of memory" error and could no longer function properly. After this, the students could no longer interact with the pilot systems due to the broken smart card. In order to mitigate this issue, the students had to contact a pilot administrator who would re-initialize their smart cards and advise them to obtain their credentials only once. This issue was reported to the consortium and a decision to use different smart cards with more processing power and storage capabilities on the second round was made.

Finally, the smart card readers that were provided to the students were the Omnikey 3021 USB smart card reader. Some students had some problems with them because the smart card reader drivers were not installed correctly (from Windows Update Manager). However, when they downloaded and installed the smart card reader drivers manually, these problems were solved.

Figure 24: A Student Swipes her SC in front of the Class Attendance System

3.9.2 Second Round

Having the experience from the first round of the student pilot, where the pilot administrators had to deal with some major smart card issues (see Section 3.6.1), it was decided to switch to another smart card platform. That is why in the second round of the student pilot, the MULTOS smart card (see http://www.multos.com/) which offered bigger memory and more processing capabilities, was deployed. This smart card could work in contact and contactless mode, as required from the pilot scenario. Moreover, the smart card processing power in combination with the fact that we lowered the key length (1024 bit) for this round of the pilot improved the overall timings for the various pilot operations (see also Section 3.8.2).

With the new smart card in place and the outcome of the first round of the student pilot, the User Client Application was modified in order to deal with cases where the smart card storage space was not sufficient for storing a new credential. This way, the "Out of memory" error was avoided and when a student would try to flood her smart card with multiple credentials, she would not be allowed to do so and her smart card could still operate normally. Moreover, in this round the User Client Application allowed the students to delete any unnecessary credentials they had stored on their smart card, in order to save memory space in case it was required (e.g. in order to get issued the tombola credential).

As mentioned also in Section 3.6.2, some minor issues regarding the smart card surfaced. More specifically, some students could not unlock their smart cards when the PUK value was shorter than 8 digits. However, this issue was a limitation of the User Client Application and could be fixed easily by the administrators who provided to the students a script for this purpose. Additionally, this issue affected some students who tried to collect attendance for the lecture while their smart card was in locked mode. For this reason, the smart card had to be unlocked first (using the corresponding script) and then the attendance units could be loaded on it.

Another issue regarding the smart card application was discovered by the pilot administrators during a series of demonstrations. When a User who had in her smart card the university and course credentials but not a sufficient attendance counter value, tried to log-in to the Course Evaluation System, her university credential state changed from 'presentable' to 'presentation committed'. When the proof failed (due to low counter) the university credential state did not change back to 'presentable'. As a result, this credential could not be used in future proofs and the student needed to re-obtain it from the University Registration System. However, this issue did not affect the students that participated in the pilot since all of them had collected the required attendance units when the Course Evaluation System was available.

Figure 25: The Omnikey 3021 USB Contact Smart Card Reader

Finally, regarding the smart card readers that were deployed in this round of the pilot, we provided to the students the Omnikey 3021USB Contact smart card reader. Since no major issues had come up with this reader during the first round, we decided to use it again. Once again, some students had some problems with the reader because the drivers were not installed correctly (when using Windows Update Manager). However, they were advised by the pilot administrators to download and install the reader drivers from the Ominkey website; the issues were then resolved. For the Class Attendance System we once again used the Omnikey 5321 USB smart card reader, which offers a contactless interface (which was required).

3.10 Stability Evaluation of the Student Pilot

3.10.1 First Round

Having completed successfully the first round of the student pilot we can conclude that the pilot was overall quite stable. The students did not experience any problems with the pilot's network and they never had any difficulties accessing the pilot systems. Additionally, the pilot administrators did not have to deal with network attacks like Denial of Service and no unauthorized access to the pilot systems was observed.

Moreover, the pilot web applications (University Registration System and Course Evaluation System) were working as expected, so the pilot administrators did not have to face any issues with them. The response time of the pilot system was a bit slow due to delays on the User side. However, these delays are acceptable considering the heavy cryptographic computations that were performed by the User Application (ABCE) and the User's smart card. Finally, the Class Attendance System was working properly and its response time was fast enough so that the students would not queue in order to collect their certified attendance units at the course lecture.

As mentioned in the previous sub-sections, the pilot administrators had to deal with some minor technical issues during this pilot. First of all, some students had problems with the installation of the User Client Application in Windows 64-bit systems. This problem was solved by providing the students with an updated installer which worked properly. A second problem regarding the Client Application was related to the Java installation (broken installation after automatic updates) on the User's PC. This issue was fixed by uninstalling Java and re-installing the User Client Application installer. Another minor issue that the students faced was the installation of the smart card reader drivers but that was also easily solved by manually downloading and installing them.

Apart from the above issues, two major technical issues were discovered during the first round of the student pilot. The first had to do with the concurrent access of the pilot systems ABCE layers. The reference implementation of the ABCE layer was not designed to be "thread-safe" at that point in time. As a result, when students tried to launch issuance and presentation simultaneously the pilot system could reply with an error response code. However, if the student re-tried to perform the procedure it would be completed successfully. The second issue had to do with the limited memory space on the BasicCard. When the students tried to obtain their credentials multiple times the smart card returned an "Out of Memory" error and could not function properly. In order to solve this issue, the students had to contact a pilot administrator who would re-initialize their smart cards.

In conclusion, although the pilot administrators had to deal with some technical issues, the pilot was completed successfully. The pilot's goal which was to give some early feedback to the project developers was achieved. The major technical problems will be resolved and fixes will be deployed in the second round of the pilot. More precisely, for the second round the ABCE layer will be "thread-safe" by design and new smart cards (MultOS) with bigger memory and processing power will be distributed to the students.

3.10.2 Second Round

The second round of the student pilot concluded successfully on Wednesday 26/2/2014. One could claim that the second round of the student pilot was overall pretty stable. Its goal, which was to deploy the new crypto architecture (offering interoperability between U-Prove and Idemix) and showcase some new features of Privacy-ABC technologies (revocation, inspection, issuance with carry over attribute) was fully achieved.

During the pilot, the network operation was quite stable. The only issues that came up were some scheduled maintenance tasks and some unexpected power failures that blocked the access to the systems for a very short time. The pilot students could reach the pilot systems at all other times without any network delays. Moreover, there were no attacks (DoS) launched against the pilot systems and no unauthorized access was observed.

The pilot applications were working as expected. The students could obtain without any problems their university and course credentials from the University Registration System. Additionally, they could get their attendance units during each course lecture as the pilot administrators would set up the Class Attendance System in the lecture room. When the semester was over, the students who had obtained their university and course credentials and had attended sufficient lectures could log-in to the Course Evaluation System and submit their evaluation for the course. Moreover, they were able to obtain the tombola credential and register for the online lottery through the Tombola System. As soon as the lottery was over, the pilot administrators along with the Inspector used the Inspector Application in order reveal the matriculation number of the winner. Throughout the pilot, the administrators did not notice any exceptions at the ABCE layers of the systems, a fact which indicates that Privacy-ABC technologies were integrated successfully. Finally, during the second round of the pilot, the newly developed (by WP4) Identity Selector which offered a more intuitive User interface was deployed.

The system response times were acceptable, especially if someone takes into consideration the cryptographic operations that are executed on the smart card. In order to make the system faster we defined the security level to 1024 bits (another feature of the new cryptographic architecture). However, the response times are not much faster than those of the first round. This is reasonable if someone considers that the pilot scenario for the second round is more complicated (e.g. introduction of revocation, presentation of both credUniv and credCourse at the Course Evaluation System).

During the pilot, the administrators had to deal mostly with usability issues. Having already experience from the first round of the pilot, it was easy to support the students regarding the problems that they had. The installer was quite stable and would set up the User environment quickly and easily. Once again, on some students' PCs the User Client Application could not communicate with the smart card through the smart card reader. This issue was related to the smart card reader drivers not being installed properly and would be resolved if the student would install them manually. Moreover, some students had some trouble logging-in the University Registration System with their One Time Password. This issue would be solved if they cleaned their browser history and cookies. Finally, some pilot participants came upon an issue with unlocking their smart card when the PUK value was shorter than 8 digits. This issue was related to the User Client Application which was programmed to deal with PUK values of exactly 8 digits long. The pilot administrators dealt with this issue by creating a script for this purpose.

The major technical issues that came up during the first round of the pilot were resolved for the second round. The MULTOS smart card offered bigger storage space and the User Client Application was enhanced in order to deal with cases where the card did not have enough space to store a new credential. Moreover, the User Client Application allowed the students to delete redundant credentials (revoked credentials or credentials obtained multiple times) from their smart cards. Finally, the ABCE layer was now designed to be thread-safe and as a result no issues with concurrent User requests came up throughout the pilot.

One technical issue that was discovered by the pilot administrators was related to the smart card application. More specifically, when a smart card which contained a university and a course credential but did not have a sufficient counter value, was involved in a proof towards the Course Evaluation System the state of the university credential would become inconsistent (see Section 3.9.2). As a result the university credential could not be used in future proofs and the student would have to re-obtain it from the University Registration System. However, this issue did not affect the pilot's students since at the time that the Course Evaluation System was available all of them had sufficient attendance units stored on their smart cards.

To sum up, the second round of the student pilot was successful. Its goal which was to deploy the new cryptographic architecture and to showcase some new ABC4Trust features (revocation, inspection) was achieved. Moreover, the major technical issues that came up during the first round of the pilot were fixed. Additionally, the experiences gained from the first round enabled the pilot administrators to deal easily with minor issues that the students came up with. Finally, the overall system was much more stable and User friendly.

4 User Acceptance of Privacy-ABCs

Although Zero Knowledge Proof technologies have been available for a long time, there has not been much adoption in mainstream applications. One of the reasons for that is that Privacy-ABCs are hard to understand for non-specialists. This motivated the student pilot to focus on the study the problem of technology adoption. Moreover the student pilot examined whether the adoption of Privacy-ABCs is a valid reason and what other factors may play a role. Even though this study falls outside of the original work plan, we decided to dedicate the extra effort for it during the project, so that we can take advantage of the Users' participation in the project to gather experimental results.

This section provides, through reporting on the execution of the two rounds of course evaluation, feedback on the User acceptance and participation of the student pilot. The focus of this section is on gathering information, from the User's point of view, on the reactions of the students that participated in the two rounds of the ABC4Trust student pilot

4.1 User Acceptance of Privacy-ABCs for the first Round

As part of this study, we made a questionnaire (see Appendix D) and distributed it to the students after the successful completion of the first round of the student pilot. In this section we present the first results from the processing of this first questionnaire. The results presented here were also presented in the research community dealing with usable privacy technologies [BKR+13]. The experience from processing this version of the questionnaire has been used to produce the questionnaire for the second round of the student pilot, as well as the second round of the school pilot.

4.1.1 Setting of the Study

Our questionnaire was distributed to the students that participated in the first round of the student pilot, after the pilot was completed. In particular, as we mentioned earlier in this document, this concerns the students who attended the course "Distributed Systems I". The questionnaire is attached at the Appendix D of this document for reference.

It is important to note here again that the 100 enrolled students of the course were given an introductory lecture on the concepts of Privacy-ABCs at the beginning of the semester. Then 48 of them decided to take part in the pilot and they were given smart cards and corresponding readers, as well as supporting material (manual, videos, etc.).

4.1.2 General Profile of Users

4.1.2.1 User Demographics

At the end of the fall semester, we distributed to the 100 course participants the printouts of the questionnaire in order to collect their opinion. The entire 100 students were able to fill in the questionnaire in their classroom as well as in their home. 55 students delivered (anonymously) in a box at a department's office their filled in questionnaires. 42 of the 55 students participated the first round of course evaluation. 42 respondents (29 male, 13 female) had used the system, and 13 (8 male, 5 female) had not used the system. The majority of the participating students evaluated the course but very few of them did not take the course's exams and therefore they did not care about course's evaluation. We distributed an additional questionnaire that addressed the comparison between the two technologies to the 6 of the 42 students who evaluated the course using both U-Prove and Idemix technologies (this questionnaire is presented in Appendix E).

These questionnaires are attached at the appendix of this document for reference.

4.1.2.2 Online Services Usage and Trust in Provider

The vast majority of the participating students use online services. The students study computer science, thus are familiar with e-services as Figure 26 shows. To measure trust, we constructed a new formative scale that asked about the trust into the different stakeholders: the developers of the system, the ABC4Trust project, the environment (University of Patras) and the underlying cryptographic algorithms (see Question 12 in Appendix D.1). The majority of participants did not distrust the system and their trust level varied very marginally between the different stakeholders (see Figure 27).

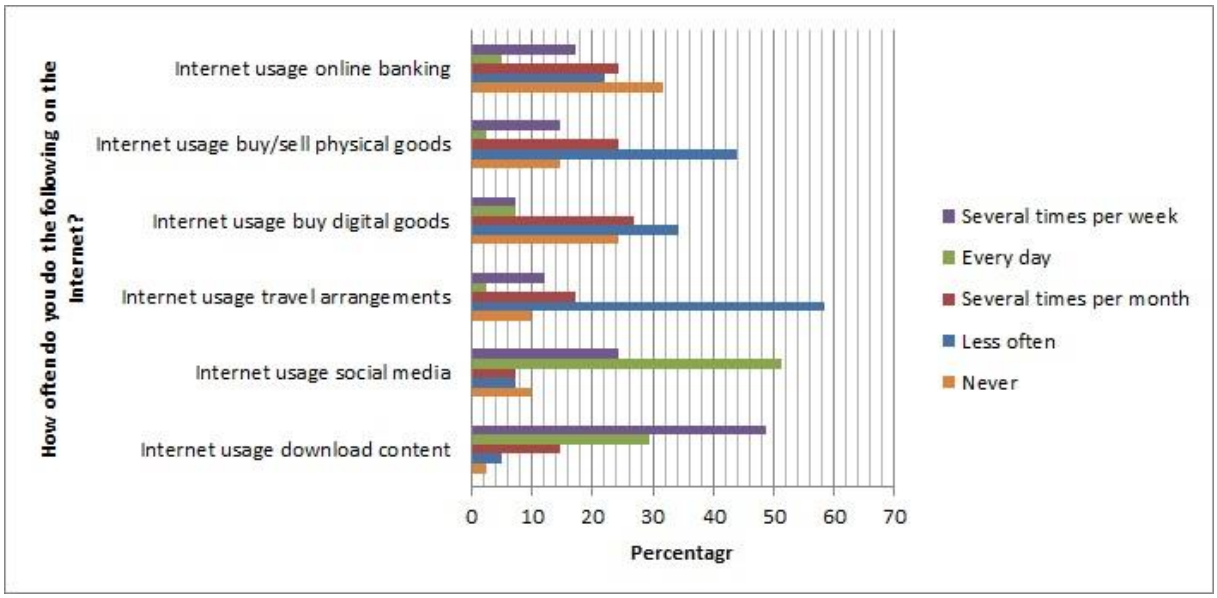


Figure 26: Internet Usage

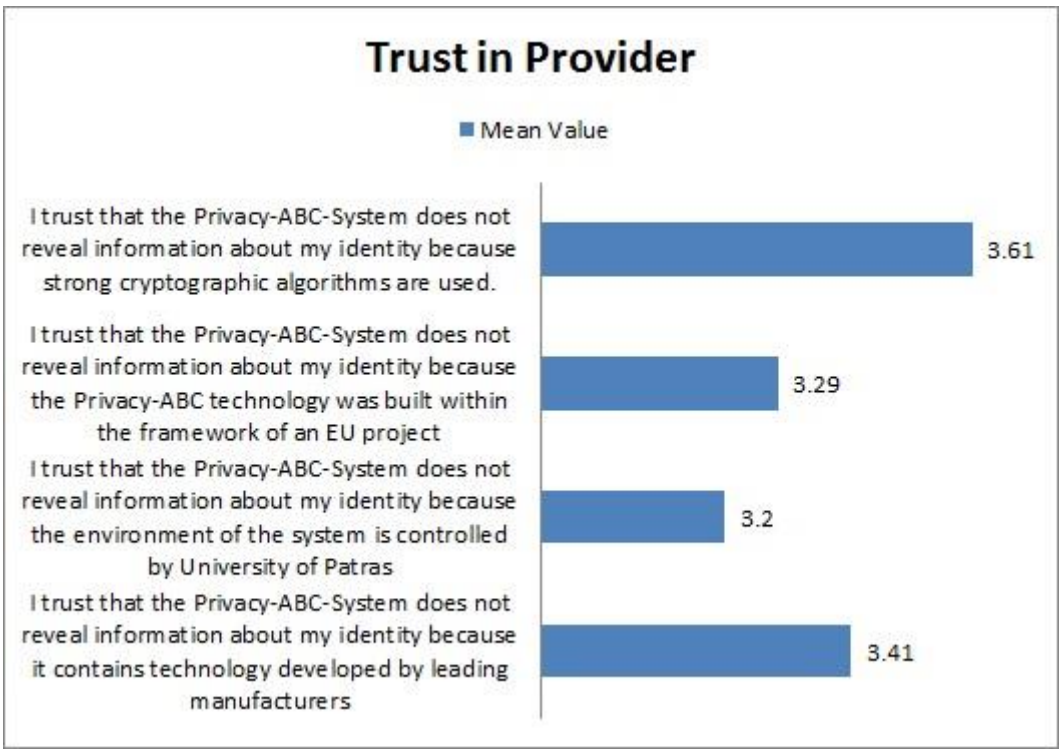


Figure 27: Trust in Provider

4.1.2.3 Privacy Concerns and Awareness

We decided also to measure Users' privacy concerns and awareness and privacy-aware behaviour (i.e., User's behaviour that protects User's privacy). We also believe that privacy awareness and privacy concerns will play an important role in the perceived usefulness of Privacy-ABCs.

Participants expressed a relatively high level of privacy concerns, as 34.1% were classified as privacy fundamentalists and the rest as pragmatics according to Westin Index [KC05]. Similarly, privacy awareness was also measured with knowledge questions about privacy issues, for example about the usage of cookies, or about connections between IP address and User's location and personal data. To measure privacy-aware behaviour, we asked the participants about their usage of different privacy protection mechanisms, such as cleaning cookies or browsing in private mode. Privacy awareness was generally high, Figure 28 shows that on average, 84.55% of the questions were answered correctly. The results of privacy-aware behaviour varied a lot between different privacy protection actions.

Figure 29 presents the results of privacy-aware behaviour, where 88% of the students responded that they sometimes clean the cookies and history from their browser, while only 29% of them have ever encrypted an email. 49% answered that they sometimes use the private mode in their browser, while 66% stated that they sometimes refrained from creating a web account or making an online purchase because of privacy concerns.

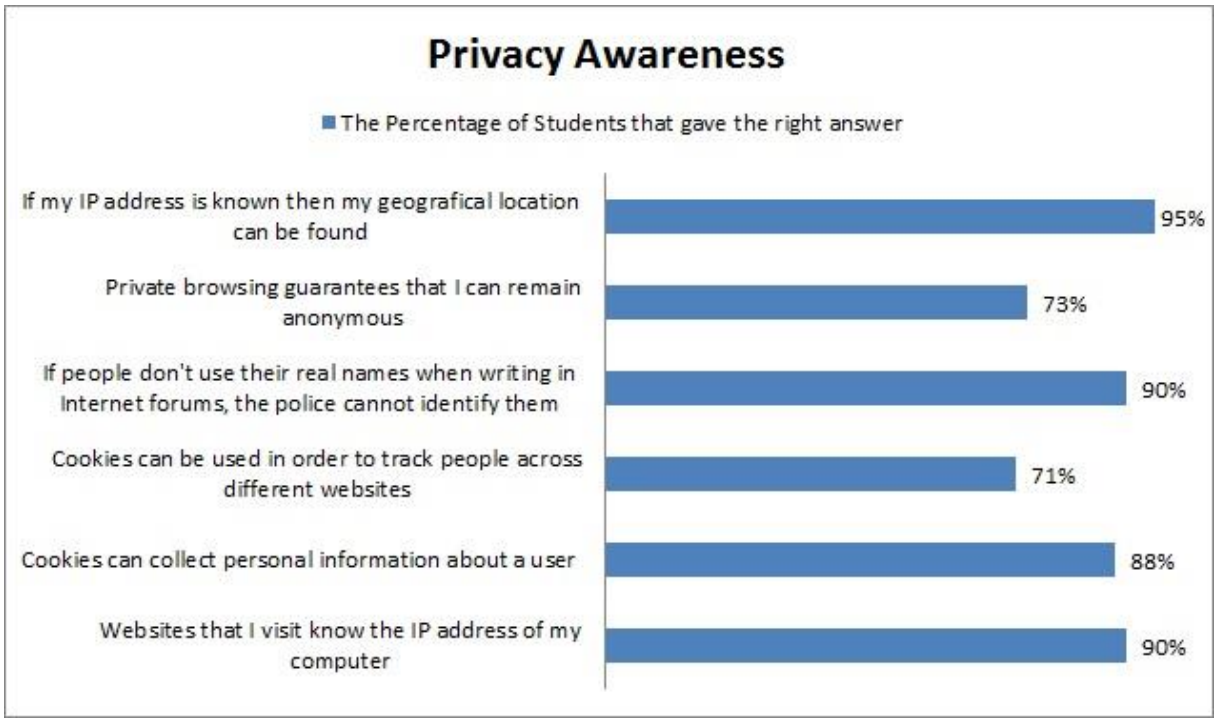


Figure 28: Privacy Awareness

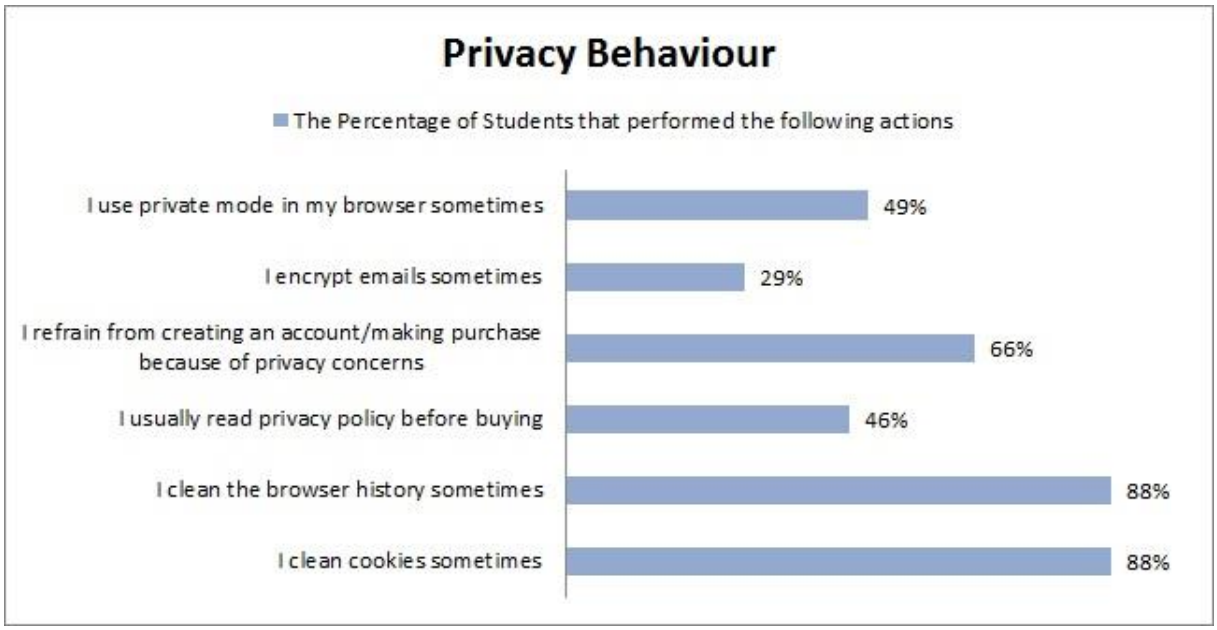


Figure 29: Privacy Behaviour

4.1.3 User Attitude towards electronic Course Evaluation

In this section we will study the concepts pertaining to the attitude of the pilot users relevant to the Privacy-ABC system as an electronic course evaluation system.

4.1.3.1 Usefulness and Ease of Use

We used the 5-item scales for *perceived usefulness* (see Question 3 in Appendix D.1.1) and *perceived ease of use* (see Question 7 in Appendix D.1.1) developed by Davis [DAVIS89].

We adopted the perceived usefulness scale to our case and asked the participants about the usefulness of the system for protecting their online privacy. The highest rank is 5, while the lowest rank is 1.

Figure 30 shows that 72% of the participating students found the system easy to use (their rate was bigger than 4) and 52% agreed that the system is quite useful for protecting their online privacy (their rate was 4). Finally the most of the students believed that understanding and usability of technology play important roles in the user adoption of the Privacy-ABC technologies. We can conclude that perceived ease of use is correlated to the intention to use the technology.

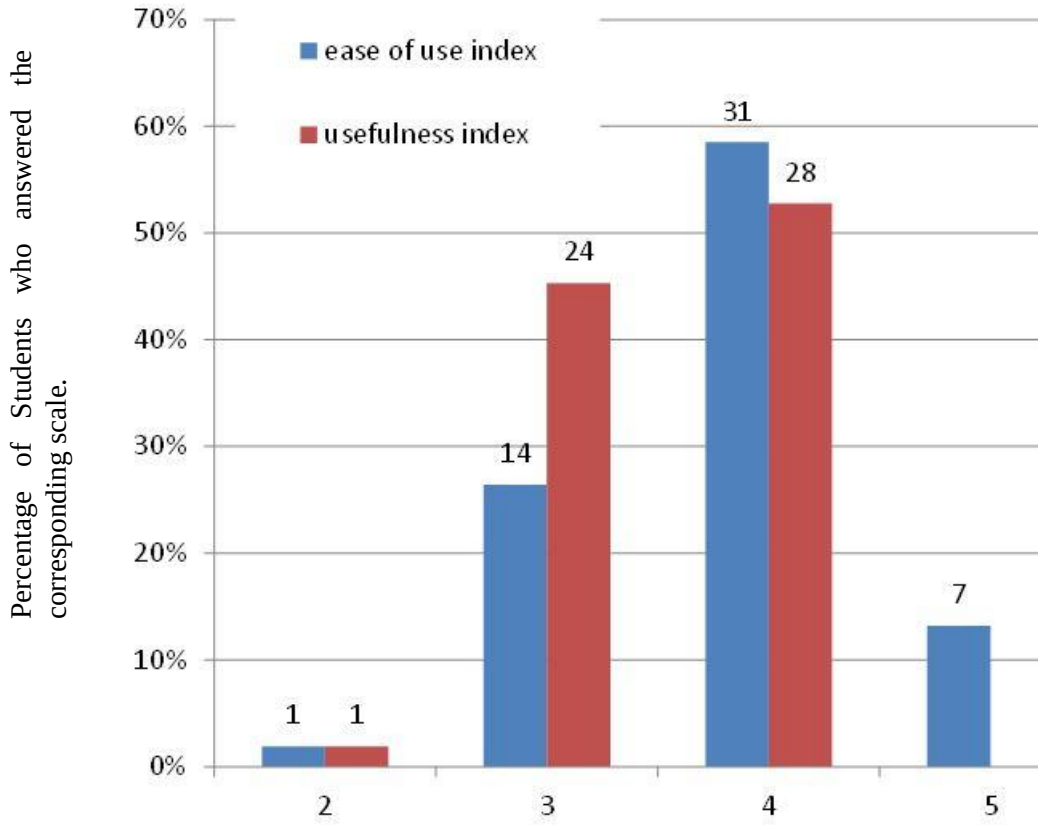


Figure 30: Perceived Ease of Use and Perceived Usefulness

One aspect of the usability of the student pilot is the involvement of a smart card that the Users had to carry with them and where class attendance data is stored. Therefore, it is important that the User does not lose the smart card. We asked the Users whether they were worried that they might lose the smart card during the semester (see Question 5 in Appendix D.1.1). Figure 31 shows that the most of the students replied that they were not or little worried about it, while 29% appeared to be more worried. The students have to make a backup of their attendance units in order to be able to restore the backed up data on a new SC. However as Figure 32 shows, only few Users stated that they used the backup tool for the smart card information during the semester and 10% of them did not know about the existence of the backup feature (see Question 4 in Appendix D.1.1).

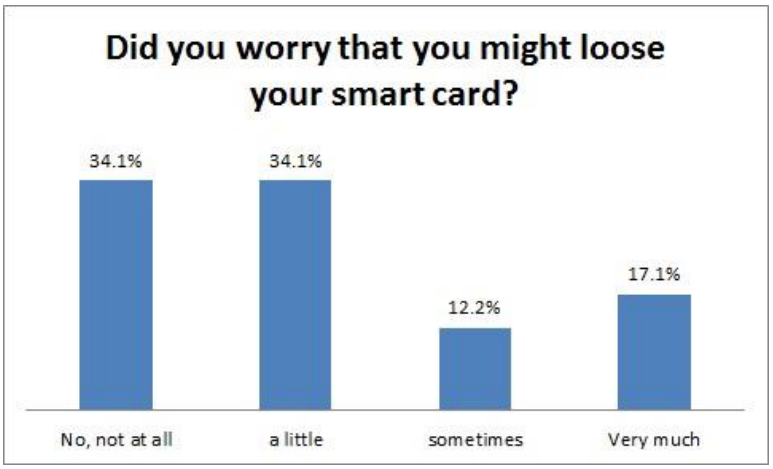


Figure 31: Worry to Lose Smart Card

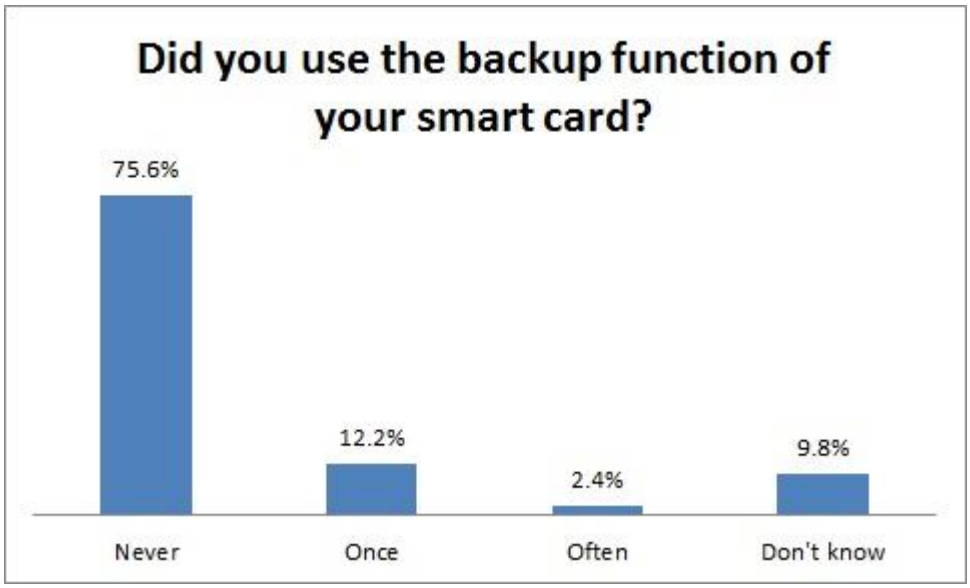


Figure 32: Use of the Backup Function

4.1.3.2 Importance and Preference of Course Evaluation

Initially, we examined if the students found interesting the course evaluation as an application scenario for implementing a new enhancing technology like Privacy-ABCs (see Question 14 in Appendix D.1). The course evaluation holds little interest for students (see Figure 33) but as Figure 34 shows the majority of them would use without reservation the course evaluation system that we developed. Moreover, we explored how useful students found Privacy-ABCs in the specific scenario of course evaluation. The students were asked if they have ever used a paper-based or an electronic course evaluation system in this or in some other university (see Question 9 in Appendix D.1.1). Figure 35 shows that 58.5% of the Users had experience with paper-based course evaluation, while only 7.3% had used an electronic course evaluation system before the trial.

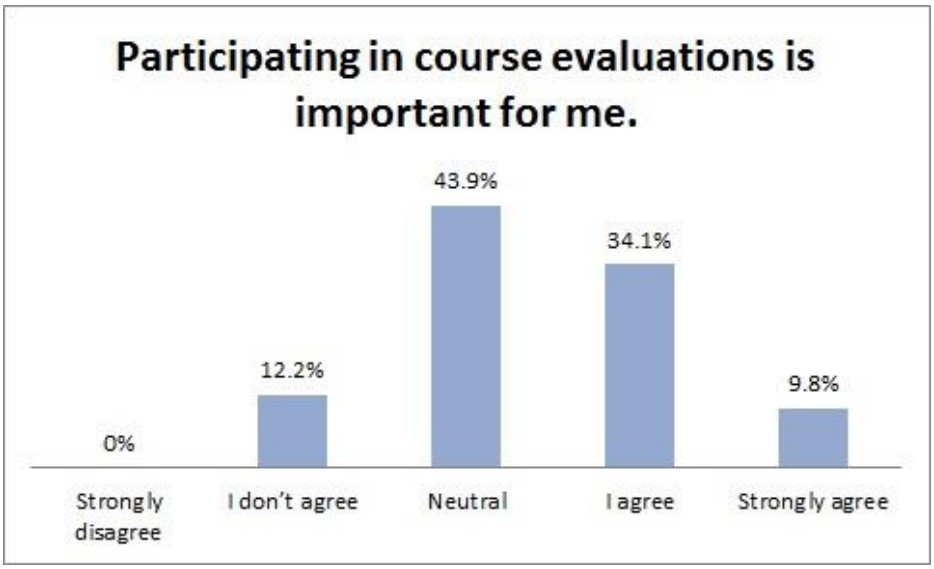


Figure 33: Importance of Course Evaluation

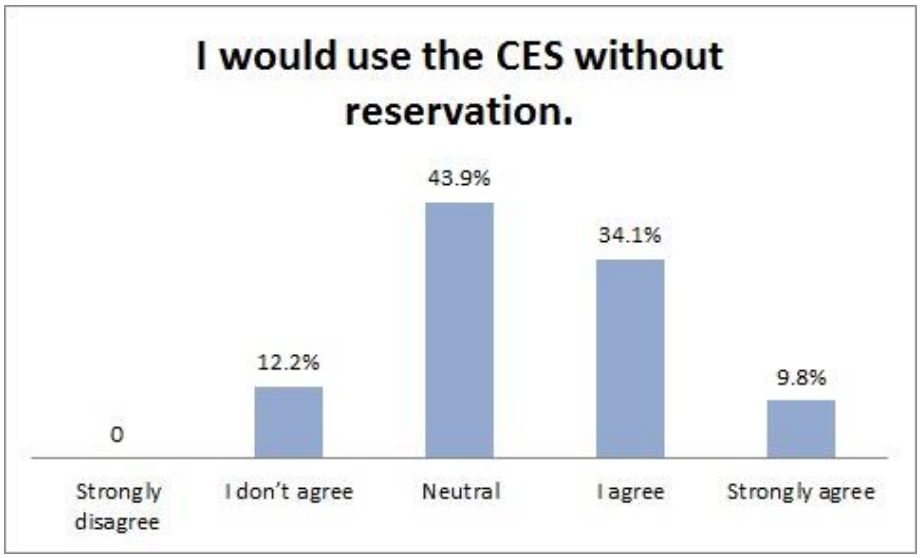


Figure 34: Intention to Use Course Evaluation System

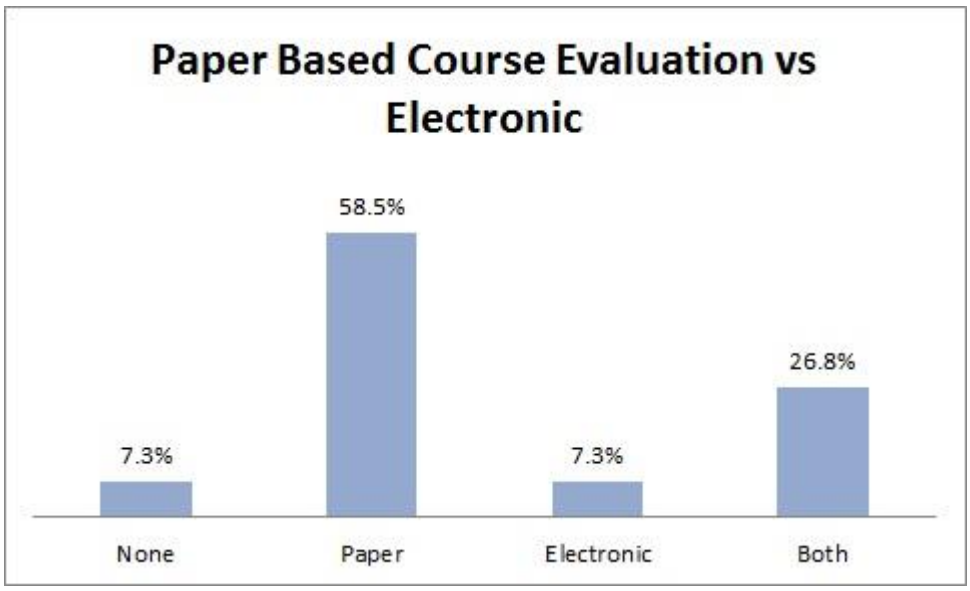


Figure 35: Paper Based vs. Electronic Course Evaluation

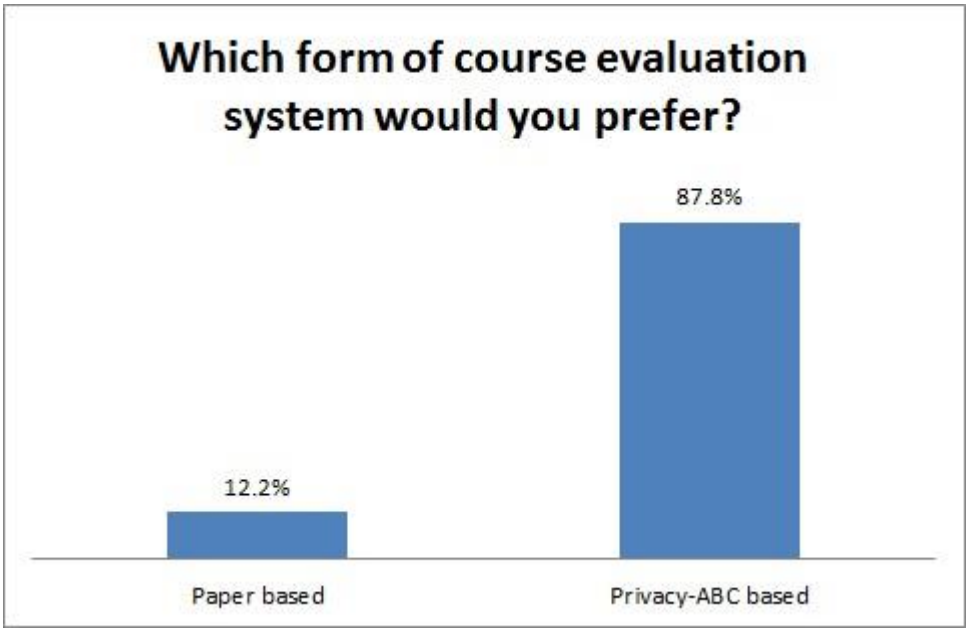


Figure 36: Paper Based vs. Privacy-ABCs based Course Evaluation

4.1.3.3 Importance of Anonymity in the Course Evaluation

The majority of students strongly agreed that protecting their anonymity in a course evaluation system is important to them. Figure 37 shows that the mean value is 4.39 and this question used a 5-point Likert scale ranging from “strongly disagree" to “strongly agree" (see Question 10 in Appendix D.1). Comparing the paper-based evaluation with the evaluation using Privacy-ABCs, students found that using Privacy-ABCs is both more convenient and guarantees their anonymity better. Eventually, Question 11 (see Appendix D.1) compares the paper-based evaluation with the evaluation using Privacy-ABCs and the students found that using Privacy-ABCs is both more convenient and guarantees their anonymity better. Figure 36 shows that 87.8% of the students declared that they would prefer a course evaluation system based on Privacy-ABCs, as opposed to 12.2% of the students that would prefer a paper-based system.

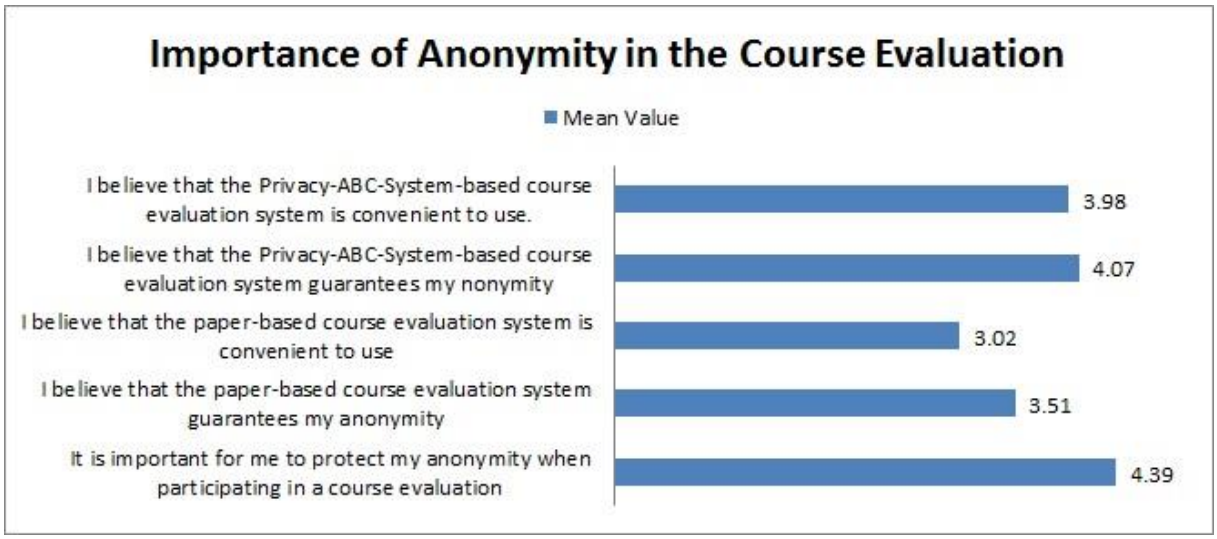


Figure 37: Importance of Anonymity of the Course Evaluation

4.1.3.4 Comparison between the two Technologies

The questionnaire which addressed the comparison between the two technologies (see Appendix E) examined if the students have noticed any differences when interacting with the student pilot's systems by using their Idemix smart card and their U-Prove smart card . Here no conclusion was driven, since at the first round of student pilot the smart cards used similar procedures for key binding for both technologies.

We distributed and collected 7 printouts of the questionnaire. The students could write down their comments in free text. As depicted in the graph below there is no specific remark noticed by the majority of the students. More precisely 1 of them stated that System's interaction was faster for obtaining the university and course credentials by using their U-Prove smart, 1 of them stated that they noticed minor differences at their interaction with system's menus or interfaces, 3 of them stated that they noticed any differences by using the two technologies and 2 of them stated that she found out her interaction with the Registration System for registering her U-Prove smart card was slower but she had a faster access to the Course Evaluation System.

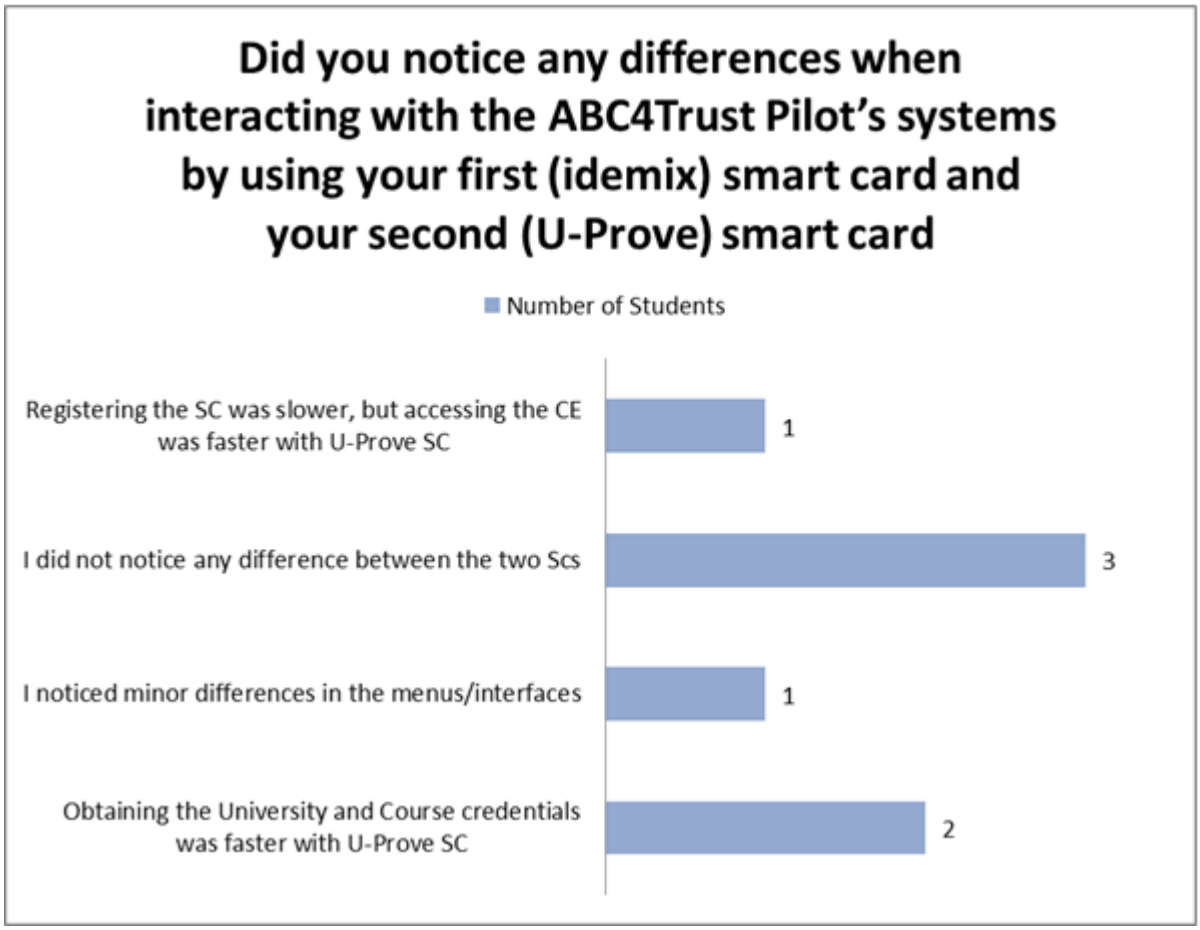


Figure 38: Comparison between the two technologies

4.1.4 User Acceptance of Privacy-ABCs

At this section we study the different user acceptance models of the Privacy-ABC technologies. At the first round of student pilot we try to analyse only the factors that influence the knowledge about the presented technology.

4.1.4.1 Understanding of Privacy-ABCs

One of the first things that we examined in the questionnaire was how well did the students understand the features of the technology they were using. In particular, we concentrated on the following main features:

- *Pseudonymity:* A student can authenticate to the system under a pseudonym and thereby disguise his/her identity in a retraceable way. No one else (including a malicious Issuer) can present a matching pseudonym to hijack the User's identity. Since pseudonyms allow a re-identification of the data subject personal data is processed and data protection rules apply.
- *Selective Disclosure:* The student is able to prove the desirable properties, e.g. verify her enrolment to the course she has registered for, without disclosing more information.
- *Untraceability*: The property that an action performed by a User cannot be traced back to her identity. In particular, the property that a presentation token generated by a User cannot be traced back to the issuance of the credential from which the token was derived.

- *Unlinkability:* The property that different actions performed by the same User, in particular different presentation tokens generated by the same User, cannot be linked to each other as having originated from the same User.
- *Consumption Control:* Students cannot submit more than one evaluation for the same course.

The understanding of the concepts underlying the Privacy-ABCs was tested using six knowledge statements that corresponded to the above concepts, such as pseudonymity, minimal disclosure or untraceability. The statements could be marked by the students as true / false / don't know. We present the distributed questionnaires in Appendix D.

For example, the statement "When I authenticate to the system, the smart card transmits its unique serial number" was designed to test the understanding that interactions with the system are pseudonymous, that is, the system cannot identify the User (and her card), and thus the serial number of the smart card is not transmitted to the system (Verifier).

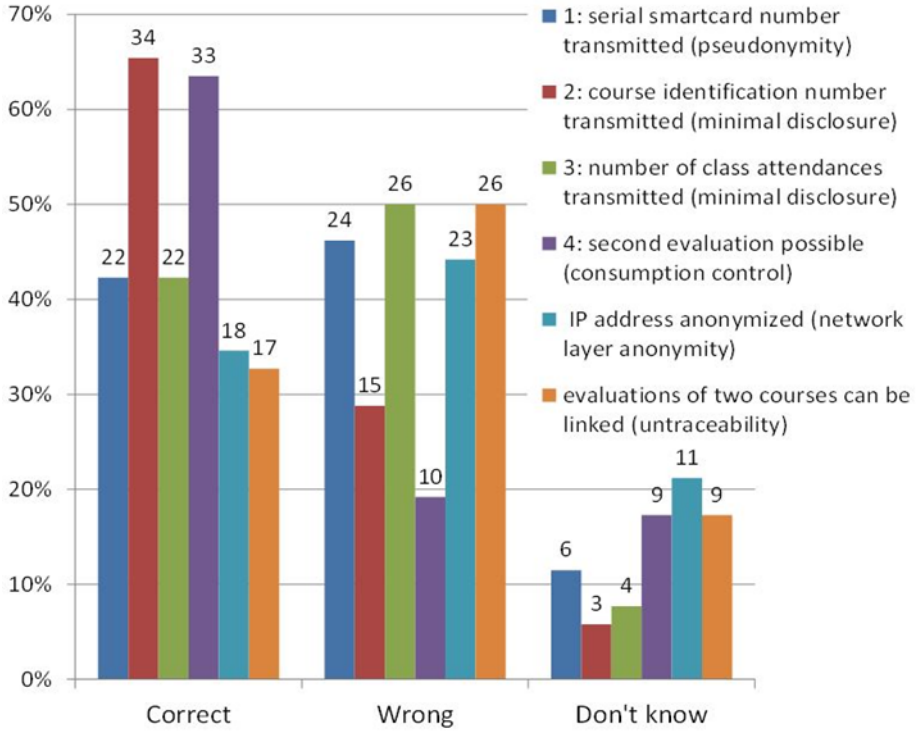


Figure 39: Understanding of the technology

Figure 39 shows the results we got from this question (for more details please see Question 2 in Appendix D.1). As one can see, most participants had difficulties with the understanding of the underlying concepts, as 4 out of 6 questions were answered wrong by the majority of the students (i.e., the students gave the wrong answer) or they were indicated as "do not know". There were no significant differences in understanding these concepts between students that used the system and students that did not use the system. It is important to note here that all 54 students were briefed on the concepts of Privacy-ABCs and they took part in several presentations on the goals and the use scenarios of the student pilot. All the 54 students have been informed in detail about Privacy-ABC technologies and they got the supporting information material so there are no significant differences in understanding between students that used the system and students that did not use the system.

4.2 User Acceptance of Privacy-ABCs for the second Round

During the second round of the pilot we distributed an updated version of the questionnaire to the participants, in order to collect their feedback on the implementation of the overall system as well as their interaction with Privacy-ABCs. We present the analysis[2] of the results into three parts. First, we show what the overall profile of the users was, including their online behaviour and their overall attitude towards privacy. Second, we study the users' reaction towards the course evaluation system using Privacy-ABCs as opposed to paper-based course evaluation. Finally, we concentrate on the overall user acceptance of Privacy-ABCs and try to understand what factors affect their adoptability by users.

4.2.1 Setting of the Study

The second round of the user acceptance for Privacy-ABCs was conducted in a similar manner to the previous round. The questionnaire was distributed to the students that participated at the second round of pilot participants. The students were attendants of the course "Distributed Systems I". The course had 60 enrolled students out of which 45 decided to participate in the pilot. Finally, 30 (23 male and 7 female) students volunteered to fill the survey. 21 of them filled the survey in their class while the rest 9 submitted it anonymously through the department's mailbox. The majority of the 45 participating students evaluated the course but few of them dropped the course and they did not take the course's exams, therefore they did not care about course's evaluation.

The questionnaire has different sections that are arranged in a convenient way to investigate the user acceptance of Privacy-ABCs particularly in the course evaluation scenario. At the second round the formal questionnaires (see Appendix D.1) was updated for collecting opinions of the students so that the questions to be more unambiguous and clear and to be referred to the new functionalities of the second round of course evaluation. The questionnaire is attached at the appendix of this document for reference (see Appendix D.2).

It is important to note here that the 60 enrolled students of the course were given an introductory lecture on the concepts of Privacy-ABCs at the beginning of the semester.

4.2.2 General Profile of Users

4.2.2.1 User Demographics

Out of the 30 students who volunteered to fill the survey, 23 were male and 7 were female. It is important to make a note that the students have computer science background and therefore they are expected to have a general understanding of online privacy and security concepts.

4.2.2.2 Online Services Usage

First, we study the participants' involvement in online activities such as online banking, online social networking, online shopping, and online storage usage by asking questions related to different online services involvements (see Question 23 in Appendix D.2).

As depicted in the graph below, the majority of them are active on online banking with 56.7% positive replies. A higher number of the students (93.3%) are even active in online storage services such

[2] **Acknowledgment**
We thank Zinaida Benenson for her help in the conceptual design of the questionnaire. We also thank Anna Girard for her help in data analysis.

Dropbox. As compared to other services (such as social networks 83.3%), the online storage services have more number of participants.

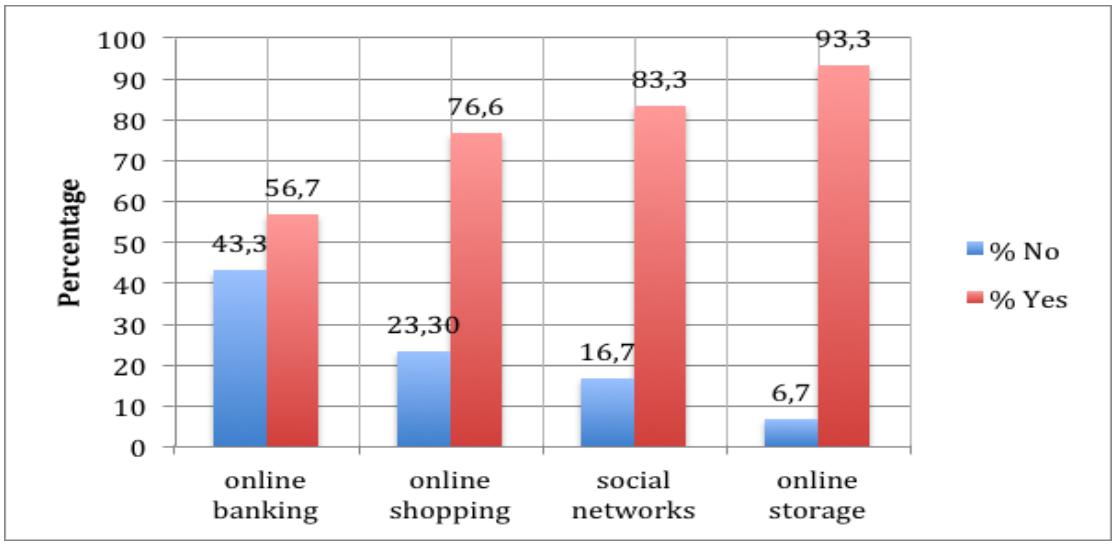


Figure 40: Users' Usage of Online Services.

4.2.2.3 Privacy Concerns and Awareness

People on the Web are generating and disclosing an ever-increasing amount of data, often without full awareness of who is recording what about them, and who is aggregating and linking pieces of data with context information, for a variety of purposes. Through the analysis of the online services usage, we have found out that the students are already active on most online services. To this end, we have included conceptual questions as part of our case study in our pilot that further resulted in an evaluation of the general perceptions, attitudes, and beliefs about privacy online. According to Dinev et.al [DINEV05], Internet privacy concerns affect the behavioural intention of Internet users to conduct online activities (see Question 24 in Appendix D.2). Perceptions of privacy are socially constructed through communication and transactions with social entities over a networked environment, a process that involves a certain level of technical skill and literacy. Their research model shows that social awareness and Internet literacy are related to both Internet privacy and intention to use online services.

According to the statistical analysis results of our study using scales adapted from Dinev [DINEV05] (the adapted scales are included in Question 24 in Appendix D.2), we understood that the majority of the students (mean=4.03, σ=0.856 on a 5-points Likert scale) are concerned about their online information misuse by other parties.

Another concept of concern to our study was the privacy awareness of the pilot participants. Privacy awareness can help users to be informed about what silently happens during their navigation while learning from disclosure of personal information may help to discriminate potential harmful activities from daily and regular activities that can be performed online. Privacy aware users tend to make informed decisions to reduce their degree of exposure and misuse of their personal information by other parties. The following table summarizes the results of the Question 25 (see Appendix D.2) which presents the privacy-aware behavior activities of the participants.

Number	Privacy-aware behavior related question	Mean	Std. deviation
1	How often do you delete cookies from your computer?	3,33	1,093

2	How often do you use private mode in browsers? (Also called privacy mode or incognito mode)	2,97	1,377
3	How often do you clean the browser history?	3,13	1,042
4	When you enter your personal information on a Web site, how often do you read privacy policies?	2,20	1,064
5	How often do you intentionally enter false information when creating a web account?	2,97	1,189
6	How often do you decide not to create a web account or not to make an online purchase because of privacy concerns?	3,13	1,137

Table 1: Privacy Aware Behavior

4.2.3 User Attitude towards electronic Course Evaluation

Course evaluations have become standard practice in most universities around the world. They are usually conducted anonymously in order to ensure credible results. Privacy-ABC technologies are employed in the pilot to guarantee that no identifying information about the students that submit the evaluations is sent to the system. At the same time, the Privacy-ABC system guarantees that only eligible students can have access to the evaluation of a course. That is, the system verifies that a student (1) is enrolled in the university, (2) has registered to the course and (3) has attended most of the lectures of that course.

Although the above conditions can be partly satisfied by paper-based and other electronic course evaluation systems, it is difficult (and sometimes impossible) to ensure all of them. For example, in the paper-based evaluation, students can be de-anonymized by their handwriting. When the evaluations are conducted through computers, the students often need to put a lot of trust into the systems and into the technical staff. In both cases, ensuring that only the students that attended most of the lectures can evaluate the course requires quite a lot of effort.

In the following sections, we will present concepts pertaining to the attitude of the pilot users relevant to the Privacy-ABC system as an electronic course evaluation system. These factors are regarded as less determinant factors in the adoption of the system.

4.2.3.1 Usability Concerns

The usability of the Privacy-ABC system for course evaluation for the students participating in the pilot was also among the concepts of focus of our user case study. One aspect of the usability of the pilot technology is the effort they exerted to setup Firefox at the beginning, as Firefox was the browser utilized for deployment (see Question 3 in Appendix D.2). Above half of the students (53.3%) didn't use Firefox as default browser before the pilot however 43.3% found it very easy to set it up. Another consideration is the involvement of a smartcard that the users had to carry with them and where class attendance units are stored. Therefore, it is important that the user does not lose the smartcard. Question 1, in Appendix D.2, asked the users whether they were worried that they might lose the smartcard during the semester. Most of them (63.4%) replied that they were not at all or little worried about it, while 20% appeared to be more worried. 60% the students were also comfortable knowing that their personal data is stored in the smart card.

Another usability relevant parameter is the help functions the students get from the system itself. Question 18 includes the adapted scales from McKnight et al. [MCKNIGHT11] and focus on the psychometric measurement of the belief that the specific technology provides adequate and responsive help for users. Accordingly, an analysis of the scales measurement in our scenario show that most participants (mean=3.88, σ=0.727 on a 5-points Likert scale) found the system providing sensible and effective advice through its help function.

4.2.3.2 Perceived Usefulness of Privacy-ABCs for Course Evaluation

The perceived usefulness of an information technology system, as defined by [DAVIS89], is the extent to which a person believes that using the system will enhance her or her job performance. As such, we adapted the perceived usefulness scales from Davis to evaluate the underlying concept as applied to the Privacy-ABC system as an electronic course evaluation system in the pilot (see Question 17 in Appendix D.2). The collected data analysis shows that many of the students (mean = 4.1, σ = 0.656) found the Privacy-ABC system useful in improving their performance and enhancing the effectiveness of their course evaluation which is attributable to the system's electronic nature especially as compared to the traditional paper based evaluation. The lower standard deviation result also shows that most students' perception about the usefulness of the Privacy-ABC system in course evaluation is similar.

4.2.3.3 Importance of Anonymity in Course Evaluation

The Privacy-ABCs as implemented in the pilot provides users the capability to stay anonymous while participating in the course evaluation. In addition to the usefulness as course evaluation, almost all students also strongly agreed that protecting their anonymity in a course evaluation is important to them (The mean value for the second item of Question 19 in Appendix D.2 was 4.57 on a 5-point Likert scale).

4.2.3.4 Privacy-ABCs Usage in Other Scenarios

Besides providing anonymity in the course evaluation, the participants were also asked open questions to suggest where Privacy-ABCs could be utilized (see Question 15 in Appendix D.2). The suggestions include online marketing, online voting, online private discussions, bank transactions and others. An analysis of the willingness of the participants to use Privacy-ABCs in other scenarios shows that 80% are ready to use it while 16.7% said no to it. The rest 3.3% have not specified their answers.

4.2.3.5 Preference: Privacy-ABC-based or Paper-based Course Evaluation

In their previous course evaluations, the majority (66.7%) of the students have used paper-based evaluations while the remaining 33.3% have not used it. While on the other hand 76.7% of them have not used electronic course evaluations systems (see Question 12 in Appendix D.2). Question 13 in Appendix D.2 compares the paper-based evaluation with the evaluation using Privacy-ABCs and almost all students (93.3%) preferred Privacy-ABC based course evaluation to traditional paper based course evaluation. This preference measurement's higher percentage is due to the fact that the Privacy-ABC system provides a usable electronic course evaluation platform on top of which it also preserves the privacy of the evaluators.

4.2.4 User acceptance of Privacy-ABCs

Different user acceptance models of technology have been proposed in the last decade most of which originate from theories in sociology and psychology. Out of all, the Technology Acceptance Model (TAM) has a major dominance in the information science society. The TAM is an information systems

theory that models how users come to accept and use a certain technology. The model suggests that when users are presented with a new technology, a number of factors influence their decision about how and when they will use it. In what follows, we will present the determinant factors affecting technology acceptance privacy ABCs that were incorporated into the final questionnaire distributed to the students.

4.2.4.1 Understanding of Privacy-ABCs and Usage of other PETs

Users' understanding of the technology plays a role in the final acceptance of the technology. As a result, we devised certain questions to investigate how the students understand the workings of the Privacy-ABC technologies specifically in the course evaluation scenario (see Question 10 in Appendix D.2). Contrary to our assumptions, some students seem to not quite well understand the technology while still the majority showed an understanding of the system. For example, to the question: *When I authenticate to the Course Evaluation System (called CES in the following), the smart card transmits my matriculation number to the CES,* 46.7% answered it correctly while 43.3% answered it wrongly. 10% of them were not sure about it. The questions are presented in the table below.

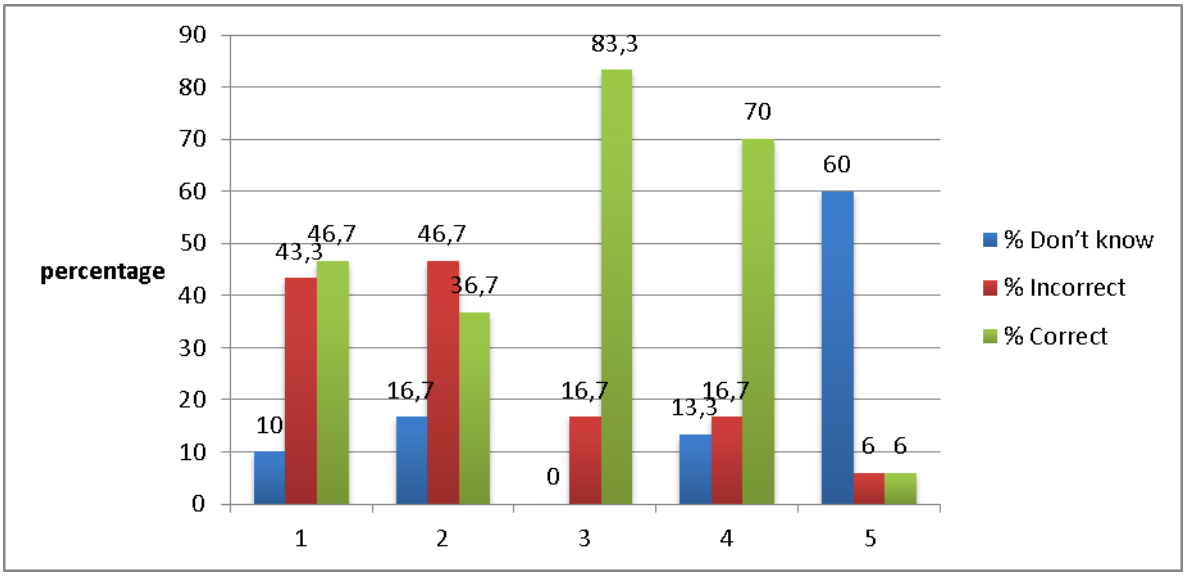


Figure 41: Understanding of Privacy-ABC System

Number	Question	Correct answer
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

Table 2: System Understanding Questions.

Part of the questionnaire also asked if the students have ever used other privacy enhacing technologies

before Privacy-ABCs for course evaluation. The analysed result showed that 83.3% have never used any PET before while the rest 16.7% have tried other PETs.

4.2.4.2 Privacy-ABCs Trustworthiness

Trust, commonly defined as an individual's willingness to depend on another party because of the characteristics of the other party [ROUSSEAU98], plays an important role in further adoption of technologies. It also plays a central role in helping information technology users overcome perceptions of risk and insecurity by making them comfortably sharing personal information and acting on the system.

In our case, how much the students trust the Privacy-ABC system is essentially investigated by incorporating trust measurement psychometric scales adapted from Pavlou [PAVLOU03] (see Question 19 in Appendix D.2). The analysis shows that the majority of the students (m=4.13, σ=0. 73 on a 5-points Likert scale) believe that the Privacy-ABC system is trustworthy.

4.2.4.3 Perceived usefulness for privacy protection

The perceived usefulness scale was originally constructed by Davis [DAVIS89] with 14 scale items. Davis later revised it and lowered the scale items to 10 items and then finally to 6 items. Vankatesh and Davis later narrowed down these to four items. The last four scale items were adapted to evaluate the perceived usefulness of Privacy-ABCs as privacy enhancing tools. Question 20 in Appendix D.2 tries to analyze the extent to which the pilot participants believe that the Privacy-ABC system will be useful in enhancing their privacy during the course evaluation. After evaluating the questionnaire, we found out that most participants found the system useful for protecting their privacy while evaluating the course (mean=3.93, σ=0.74484 on a 5-point Likert scale). The majority of them (33.3%) have graded 4 out of 5 scale measurements for the usefulness of the system in protecting privacy during the course evaluation while 20% graded 5 out 5 for the same scale.

4.2.4.4 Perceived ease of use

Question 16 in Appendix D.2 includes the perceived ease of use scale, which has also gone through similar model maturity as that of perceived ease of use since it first appeared in Davis [DAVIS89] publication. This concept is defined as the degree to which the technology (IT service system) is regarded as easy to understand and operate with-out having to exert extra efforts from the user side. The perceived ease of use of the system has an impact on the final technology adoption phase. In addition, it has been noted in technology acceptance research that perceived ease of use has direct and indirect effects towards behavioral intention. The learnability and easiness to use of the Privacy-ABC system was, therefore, analyzed by adapting the constructs from the last Davis scales. The empirical results show that most participants found the system easy to use (m=3,833, σ=0. 651 on a 5-points Likert scale).

The last 2 items of Question 20 in Appendix D.2 measure the reliability of the Privacy-ABC system and the students' reaction based on their experience. The results show that most of the students (mean=3.97, σ = 0.718) found the system to be reliable, dependable and doesn't malfunction.

4.2.4.5 Perceived risk

Technology acceptance is also affected not only by the positive utility gains attributable to system but also the negativity feeling about the system. As such, the perceived risk feeling of the system by the users was also analysed by adapting measurement scales from Pavlou [PAVLOU03]. The risk factors evaluate the potential loss feeling of the students attributable to Privacy-ABC system. The perceived

risk feeling of having one's personal identity or information misused by third parties can deter users from using the system thus affecting its adoption negatively.

The third item of the Question 19 (see Appendix D.2) measures students' perception of risk as to how they might feel when they decided to evaluate the course using the Privacy-ABC system. The options were ranging from (1=strongly disagree, 3=neutral, 5=strongly agree). The analysis shows that majority of the students (mean = 1.8, $\sigma = 0.997$) showed a lower risk perception i.e they disagreed to the presence of risk.

4.2.4.6 Perceived Anonymity

At the core of ABC4Trust project is the provision of anonymity to the students when evaluating the course. Absolute user anonymity in online services can easily lead to fraud. However, Privacy-ABCs give a balance of anonymity for honest users and accountability for misbehaving users through a feature called inspection. The inclusion of the perceived anonymity concept to our user study allows us to empirically evaluate the sense of anonymity the students perceive while evaluating the course. Question 22 asks the students if they obtain a sense of anonymity when they evaluate the course by using Privacy-ABCs (see Appendix D.2). Understanding how anonymity is perceived by the participants and how they feel about it is a vital issue that affects the final adoption of a privacy enhancing technology such as Privacy-ABC system.

The statistical analysis show that almost All students (mean = 4.2, $\sigma = 0.46$) strongly felt a sense of anonymity and the feeling that Privacy-ABC system is able to protect their anonymity when they evaluate the course.

4.2.4.7 Behavioral Intention to use

The behavioral intention to use is the other psychological construct mainly used to estimate if the users would like to continue using the system. It has fist been posited by Davis as a construct mainly affected by the determinant concepts of perceived usefulness and perceived ease of use. Behavioral intention to use also mediates the perceived usefulness and actual system use. As the students perceive the Privacy-ABC system to be useful, this consequently influences their behavioural intention to use the system. Further their perceived ease of use influences perceived usefulness leading to behavioural intention to use and ultimately leading to actual system usage.

Question 14 (see Appendix D.2) uses the last Davis scales to measure if the students would like to continue the using the Privacy-ABC system if it were to continue. The empirical analysis shows that almost all students (mean = 4.34, $\sigma = 0.59$) would like to continue using the Privacy-ABC system in the future.

4.3 Discussion and Future Work

Similar to that of the first round study, the second round survey work has several limitations that make it difficult to generalize results. For example, all participants are computer science students, meaning that they are technically savvy and interested in technology. With other User groups, especially the results on ease of use might be quite different. Moreover, the pilot system was not actually designed with usability in mind. Better usability might have improved the understanding of system properties, as showed by Wästlund et al. [WAF12].

In Section 4, we presented the descriptive statistical results on Users' understanding and usage of Privacy-ABCs. We have also measured many other variables, such as privacy awareness and concerns, or patterns of the Internet usage. The general impression is that even though the students have background in computer science, the analyzed statistical results show that some of them have

difficulty understanding how the Privacy-ABCs work while protecting their privacy during the course evaluation. Nevertheless, the other results such as usefulness, ease of use, trust and other measurement concepts show that majority of students are interested in using the system. Given the privacy enhancement they perceive, most students also preferred Privacy-ABCs based course evaluation over the usual paper based form.

4.4 Acknowledgment

We thank Zinaida Benenson for her help in the conceptual design of the questionnaire. We also thank Anna Girard for her help in data analysis.

5 Legal Considerations

This section will elaborate about general legal consideration which played a role in preparing and executing the student pilot. This entails considerations about the difference between anonymity and pseudonymity, the data subject's rights, and the deletion of personal data no longer needed after the runtime of the pilot.

5.1 Anonymity and Pseudonymity

In the context of Privacy-ABCs, and in particular when a system includes an inspection feature, the concepts of anonymity and pseudonymity become of utmost importance. With the utilization of advanced cryptography, enabling Users to retain their privacy a false feeling of anonymity might be experienced in online interactions. The situation becomes even more obscure when the general understanding of these concepts clashes with very precise legal definitions of these terms. Consequently, it seems necessary to elaborate on this topic in more detail for two reasons; firstly, when setting-up a data processing it has to be in compliance with data protection laws. Therefore, the exact legal boundaries have to be understood. Secondly, as shown above, a valid consent of a data subjects presupposes that adequate information was provided. This, however, includes that all concerns regarding anonymity and pseudonymity have to been addressed.

In general, data protection laws are only applicable if personal data is processed and personal data, in its legal sense, is understood as *any information relating to an identified or identifiable natural person.*[3] From this definition two important conclusions can be extracted. Firstly, anonymized data is not categorized as personal data. Secondly, however, the threshold for categorizing data as anonymous is very high. One can see that it is not necessary that a person is identified but identifiable. And *to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used (…) by any person to identify the said person.*[4] However, which means are reasonable can only ascertained on a case by case basis. The Article 29 Data Protection Working Party, however, considered IP-addresses or location data as personal data because it was possible to identify a person with reasonable means.[5] Consequently, whenever a re-identification is possible data is not anonymized but only pseudonymised and therefore pseudonymisation can be defined as '*disguising identities in a retraceable way.*'[6] Moreover, further encryption of pseudonymised data does not change this conclusion because encryption does not change the nature of the data even though it might technically protect it.

When applying those definitions to the data processed during the pilot, the following can be concluded:

- Without a doubt, the data transmitted from the university classroom to the university registration system constituted personal data since it included the name and matriculation numbers of the participants, as well as the courses the participants were enrolled in. Consequently, identification is possible without any major effort.
- A more complex issue is the categorization of the credentials stored on the smart card. In this context, the term 'credential' means a list of certified attributes inside a digital container.

[3] Art. 2 a) Directive 95/46/EC
[4] Recital 26 Directive 95/46/EC
[5] Article 29 Data Protection Working Party; *Statement of the Working Party on current discussions regarding the data protection reform package*, Brussels, 27/02/2013.
[6] Ibid.

Obviously if such attributes are themselves identifying a person, then the credential is personal data too, since the technical form does not change the nature of data. However, the credentials used in the pilot only certified that a person was a student at Patras University and that he/she had registered for a particular course. Nonetheless, it was possible to revoke those credentials, for example in case a participant dropped out of the course, left the university, cancelled the pilot, or lost the smart card. Therefore, there was a technical linkage between the credential and the identity of the participant. Consequently, those credentials constituted personal data. This can be noticed in particular in regards to the inspectable tombola credential which was issued by the course evaluation system after the evaluation was completed. For this purpose, the course evaluation system did not learn the matriculation number but passed it on in encrypted format to the new credential. Consequently, the credential contained the matriculation number and it was possible to decrypt the winners' matriculation number after the final drawing. A similar procedure was employed when obtaining class attendance units. Each visit of a lecture was certified by a personalized class attendance credential which was stored on the smart card of the participant. The credential included the course name, the number of the lecture as well as the hidden matriculation number, which was received from the presentation token, and thus constituted personal data.

- Finally, the results of the course evaluation did not constitute personal data. Technically, the results from the evaluation form were not linkable to the participating student. However, to prevent that the information provided in a particular evaluation would be linked to an individual student in some other way certain additional safeguards were in place. Thus, the lecturers were only granted access to the cumulated results after the evaluation had finished. Furthermore, while chances for a successful attempt to identify a student submitting a particular evaluation are minimal, it might have been possible if not enough students had submitted their evaluation. Therefore, lecturers were only permitted to view the cumulated results of the evaluation, if at least 5 students had provided feedback for the lecture.

In conclusion, a data processing operation which entails inspection must not assert that the authentication is "anonymous" as it is in fact "pseudonymous" in legal terms. To prevent misunderstandings, the activities of the User should be called pseudonymous or be labelled as 'unidentifiable under normal circumstances'. The latter term describes the core purpose of inspection quite accurate since it enables a revelation of one's identity only under strictly predefined conditions about which the User is informed in advance. Moreover, it ensures that the standard operation of the Privacy-ABCs system is by default protecting the privacy and identity of the User. Correlating with this, the User Interface of the online Privacy-ABCs system shall reflect this protection by ensuring the awareness of the Users through the provision of easily accessible information about the inspection process itself as well as the correlating inspection grounds. This can be realized by the aforementioned multi-layered approach of informing the User by integrating links to further information into the User interface or the consent form. Nevertheless, the obligation to inform is only met if the User can learn more about the inspection feature without any effort.

5.2 Data Subjects' Rights

Furthermore, like in every data processing, the issue of data subjects' rights had to be addressed. In Chapter C (Article 11 -14) of the Greek Data Protection Law the right to information, the right to access and the right to object are stipulated. To comply with these obligations and to guarantee an effective way of exercising the rights the information sheet entailed the contact details of the data controller itself, as well as the responsible contact person. Moreover, all the following possibilities were explained to the participants in the information sheet, as well as the consent form.

The right to information (Article 11 Data Protection Law) was complied with by the initial information sheet, the consent form and the User manual. Since a valid consent presupposes that all

the relevant information is provided to the data subject before he or she agrees this obligation and the obligation arising from Article 11 are not only closely linked but overlap mostly.[7] Therefore, no additional information was necessary after providing the initial information.

With respect to the obligations set out in Art. 12 and 13 Data Protection Law – namely the right to access and the right to object – it has to be differentiated between two sets of data – the personal credentials and information of class attendance stored on the smart card and the personal information stored in the registration system. We offered the participants the possibility to exercise their rights without any involvement of the data controller as much as possible. Therefore, the personal credentials were stored on the smart card of each User and protected by a PIN known only to the participant. The correlating 'Client Application' which ran locally on the computer of the User allowed her to browse, delete, or locally backup the Privacy-ABCs stored on the smart card. Nonetheless, it was necessary to store the second set of data in a central database – the university registration system – operated by CTI. However, even though the data was stored centrally, the participants had the possibility to access and rectify data online. Only if they chose not to use this possibility, were they able to contact CTI to request access or rectification. Furthermore, lecturers were also able to access their personal data gathered by the system. However, data such as the name of the lecturer and the title of the class could have been rectified only by notice to the data controller (CTI).

Last but not least, it was possible to revoke one's consent to the data processing at any time by notice towards CTI or the aforementioned contact person.

5.3 Data Deletion

Last but not least, complying with one's right to privacy and the correlating principle of data minimization requires that personal data is deleted as soon as possible after the purpose of the data processing is accomplished. Accordingly Article 4 1d) Data Protection Law stipulates that personal data should not be kept any *longer than the period required (…) for the purposes for which such data were collected or processed.* However, the Greek Law also permits that data is stored for a longer period of time for historical, scientific or statistical purposes.

In the context of the student pilot different sets of data have to be distinguished since they correlate with different deletion dates. The personal data collected to conduct the tombola was deleted immediately after the tombola had concluded and the prize had been given to the winner. Other personal data that had been processed and stored in the course of the pilot will be erased 6 months after the end of the pilot. The signed consent forms will be kept until 6 months after the end of the project. Last but not least, some of the data will be anonymized for research purposes since the pilot was part of a scientific research project. Therefore, some aggregated and anonymized data will be used to complete the research work of the project and might be used for further academic purposes, like the publication of scientific proceedings, statistics or evaluation charts. Moreover, the results of the online evaluation will also be kept in an anonymized form as well as provided to the Hellenic Quality Assurance Agency for Higher Education (HQAA) in accumulated form.

All these different time periods were openly communicated to the participants in the information sheet and the consent forms.

[7] Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR),* Adopted on 15 February 2007, (WP 131 00323/07/EN), p. 9.

6 Recommendations

In order to introduce Privacy-ABCs technologies in an application, firstly, the application scenario and their privacy requirements must be defined. As soon as the scenario is well-defined and finalized the ABC4Trust language framework can be used in order to create the credential specifications and the issuance/presentation policies. One needs to keep in mind that introducing redundant the features in the scenario (attributes in credentials that are not really required or privacy features that will probably not be used) adds a possibly undesired complexity to the overall system. The university and school pilots were the first attempts that research on operation, interoperability, User acceptance, and so forth can be conducted in a real life environment. One of the great benefits of the student pilot was that the gathered experience of student pilot provided feedback for enhancements. This feedback demonstrates issues and considerations that must be taken into account by anyone who wants to develop a similar system and are discussed in the following sections.

6.1 Revocation and Inspection

Initially, we refer to the optional Privacy-ABC technologies' features of revocation and inspection. One should introduce revocation in a Privacy-ABCs scenario, when there is the need to invalidate credentials in the system (e.g., when a student graduates from university, her university credential should no longer be valid). The existence of the Revocation Authority introduces some complexity (processing and network delays) to the overall system i.e. the Revocation Authority must be online 24/7 since when a presentation is made the Users/Verifiers need to obtain the latest revocation information. Moreover, an Inspector should be introduced in cases that there is the need to de-anonymize a presentation token e.g. identify the winner of an anonymous lottery or identify a spammer in an anonymous chat. The inspection grounds (i.e. under which conditions should inspection take place) as well as the inspection procedure should be defined in detail when the scenario is designed.

6.2 Attendance Data

Regarding design decisions, for the student pilot the project consortium had to consider the way the students would collect attendance units at the course lectures. Firstly, a Privacy-ABC solution was examined. With this solution the students would collect an attendance credential for each lecture they attended by the Class Attendance System (which would play the role of an Issuer). However, such an approach would increase the complexity of the system. In the classroom the students would queue up in order to obtain their attendance credentials and at the end of the semester the proof towards the Course Evaluation System would be too complex (combining multiple attendance credentials). That is why we chose a more simple, secure and efficient solution outside the scope of the Privacy-ABCs. Each smart card would contain an attendance counter which would be increased every time the student swiped it in front of the Class Attendance System. At the end of the semester, the smart card would allow the student to present her course credential only if her attendance counter had reached the pre-defined threshold.

6.3 Reference Implementation

From a technical point of view, integrating the Privacy-ABC technologies to a new application is quite easy. The ABC4Trust project has made the code of the Reference Implementation publicly available

on Github (please visit https://github.com/p2abcengine/p2abcengine) along with instructions of how to deploy it. The Reference Implementation implements the ABC4Trust API which offers all the necessary services for setting up the entities of a Privacy-ABC system i.e. Issuer, Verifier, User, Revocation Authority and Inspector. Of course, these services have to be integrated in the newly developed applications, a task which requires a reasonable amount of technical work and implementation.

6.4 System Testing

One basic lesson learned from the student pilot, is related to the overall system testing. Before a system is ready to go live, it is very important to perform a very extensive and detailed system testing. Additionally, it is crucial that the testing is done by people different than the developers who pretty much know what to expect from the system and how it operates. Such a procedure will help to eliminate possible bugs in the applications, which could not be predicted during the development phase and make the system more stable.

6.5 User Interfaces and System Response Time

The student pilot indicated that a critical matter for the success of a Privacy-ABC system is usability, since the perceived ease of use is correlated to the intention to use Privacy-ABC technologies (see Section 4.1.3.1). As it was perceived by the pilot participants, usability can be evaluated by two basic factors: User interfaces and system response time.

Regarding the User Interfaces, a User of a Privacy-ABC system needs to have an overall good understanding of what is happening when she interacts with it. That is, she should understand which systems know what information about her, she should be informed about what attributes she reveals or not during a proof and she should be able to give her consent when personal information is disclosed. Additionally, she should be able to browse her credentials and her personal information that is stored on her PC or security token that is used. For these reasons, during the student pilot we deployed some software that runs on the User side called *Identity Selector*. This piece of software is included in the ABC4Trust Reference Implementation and its implementation is meant to be generic, meaning that it can be used for any application. However, the student pilot results show that even so, the Identity Selector should be adapted to fit specific application needs depending on the User's needs, age, technical background, etc. Finally, the application designers should consider whether the overall interfaces should be localized (i.e. translated in the local language of the targeted Users) in order to be more friendly for the Users. Such a decision would require the application designers to adapt the credential attributes and the issuance/presentation policies to the target language as well as localize the web applications (interfaces, database entries, etc.).

The system response time is affected by various factors including processing time at the User side (User Client Application), possible network delays and processing time at the server side. As suggested earlier, the application scenario and its complexity affects the response time of a system. That is why, the application and its scenario must be designed cleverly and be practical for their purpose (e.g., introducing revocation adds complexity to the system and its response time is affected). As soon as an effective scenario for the target purpose has been defined, the system response time can be improved with some technical work. As an example, we mention that for the student pilot operations, one bottleneck was the arithmetic operations executed on the smart card. For this reason, it was decided by the consortium to lower the cryptographic key length from 2048 to 1024 bits.

In the student pilot, it was noticed that the system response time affected the User interfaces. Especially, in case that there was some processing delay (e.g., when the smart card was performing some arithmetic computations that required a few seconds) the User should be informed about it through the User Interface. This way, the User would be aware that the system is doing some

processing/computation and has not crashed. Due to the delays that were caused by the smart card operations on the User side, a "spinning wheel" was introduced to the web applications. This indication would let the User know that the system is still working and that she should wait for the operations to complete until she would get a notification whether the issuance/verification was successful or not.

6.6 Storage Devices

As far as security tokens are concerned, the use of a smart card is suggested. As a tamper proof device it offers security and it is the ideal hardware token for storing the User's device key. Additionally, it features a cryptographic processor which can be utilized for performing the cryptographic operations (exponentiations etc.) that are required during issuance or presentation. Finally, it makes a User who stores her personal data on it, more confident and trustful. During the two rounds of the student pilot, different smart card platforms were deployed. In the first round the ZeitControl BasicCard was used whereas in the second a MULTOS smart card was deployed. Despite the fact that the smart card was difficult to debug and many technical issues were discovered, it worked out well in both rounds. The technical issues that were discovered in the first round of the pilot helped the project developers to make the smart card application much more stable for the second round. As a result, the ABC4Trust-Lite smart card application is mature and can be used in future Privacy-ABC applications. If an application designer would like to avoid the deployment of smart cards for her application, then other storage areas could be considered for the User credentials. One practical alternative would be the User's mobile phone. Current mobile phones offer strong processing/storage capabilities and could assist the User for the computation of the arithmetic operations required for Privacy-ABCs protocols. Moreover, a User always carries around her mobile phone and would be careful not to lose it. However, there is the issue of where the secret key would be stored. It would be ideal if mobile phones were equipped with Trusted Platform Modules (TPMs) that could be utilized by their owners. Another alternative would be for the Users to store their credentials on the cloud. Then there would be no need for them to carry around hardware tokens. However, this requires strong authentication towards the cloud services.

Finally, another issue regarding the hardware token used is related to the information that is stored on it. When designing an application one should consider what information is stored on the token and whether this information can be retrieved again from another system e.g. in case of device loss. If that is not possible, the application designer should consider the backup/restore functionality. As an example, we refer to the lecture attendance units that the students obtained from the Class Attendance System. Since these data were only stored on the student's smart card, a backup functionality was provided to the student through the User Application. However, when considering the backup functionality for a hardware token, one should keep in mind that security issues might arise (e.g., backing up the smart card sensitive content only in cipher text etc.) and has to modify the application in order to deal with them.

6.7 University Administration

In this section, we present all the involved parties from the Greek university at the student pilot, their role, their opinions and their actions.

6.7.1 Opinions and Actions of the University Members

At the beginning of the first round of the student pilot we tried to introduce the concepts of Privacy-ABC credentials and the goals of the pilot to the community and administration of university.

Initially we tried to collect the professors' opinions for the course evaluation with regard to several usage criteria of the concept of the Privacy-ABC technologies. We presented the detailed description about the distributed questionnaires and the professors' feedback in D7.1 [ADFS12]. In general professors found the course evaluation pilot quite appealing and they found Privacy-ABC technologies interesting. They believe that Privacy-ABCs systems can change their everyday life. Although their trust level for previous evaluation methods is good, their trust level for the anonymous evaluation process is even higher. Moreover, professors preferred a course evaluation system where different questions are presented to students according to course material and their course attendance and performance. Their main concern is the impact that the results of the evaluation process will have on the course improvement. Finally, most of the professors believe that the evaluation results should be accessible from university's personnel.

Moreover all the course evaluations are supported by the Hellenic Quality Assurance Agency for Higher Education (HQAA). HQAA ensures the transparency of the course evaluation procedure and also guarantees that these procedures will be used in enhancing the quality of higher education thus we cooperated with HQAA for several activities, more precisely:

- The HQAA cooperated with the department in order to distribute a general template of course evaluation questionnaire to the professors, then each professor customized the course evaluation questionnaire to suit the course's needs.
- When the evaluation procedure was completed, CTI members collected and processed the evaluation results in order to provide accumulated course evaluation results to HQAA. Moreover, HQAA cooperated with the department for the dissemination of the evaluation results.

Finally, the student pilot took place in the Computer Engineering and Informatics Department of the University of Patras in Greece. Therefore the student pilot had to be adjusted according to the needs of the department. The role of the department was critical for the success of student pilot, more precisely:

- The Department's Registration Office employees were responsible to provide a document containing a list of participating students together with department related data.
- Only the university registration office employee could make a request to the revocation authority in order to revoke a student credential. This may happen when, for example, a student graduates from the university or upon student request (smart card loss).

Appendix A Consent forms for Students and Lecturers

Consent form for the Student Pilot in the ABC4Trust project

This consent form addresses you as a participant in the second round of a Privacy-ABCs system at Patras University within the EU-funded research and development project ABC4Trust. During this trial, your personal data will be collected, stored and processed by the Computer Technology Institute and Press "Diophantus" (CTI), "D. Maritsas" Building, Nikou Kazantzaki street, University Campus of Patras Rion. For this, CTI kindly asks you for your written consent to process the personal data listed below. For an explanation of the system deploying Privacy-ABCs which will be tested, and the type of personal data processed for which purposes, please refer to the information sheet handed out as attachment to this form. Further information about the technical specifics can be found under the project website (www.abc4trust-project.eu), and especially in the User manual that is provided online at:

https://ces.cti.gr/Portal/Portal.html

You agree that Patras University provides CTI with your Name and Matriculation number and the information that you are student at the university and that you have registered for " Distributed Systems I".

All information provided by you regarding yourself will be stored securely and will not be used or disclosed to third parties without your explicit consent. Your opinion about the lecture which you provide as part of this trial will not linkable to your person for CTI or the lecturer. For academic purposes, like the publication of scientific proceedings, reports, or presentations anonymized and aggregated graphs and statistics will be made publicly available. The aggregated evaluation results may be used and published in project reports, scientific papers, presentations or other publications. This consent form will be securely kept with CTI until its deletion 6 months after the end of the project.

Once you finish the course evaluation you may choose to enter a tombola. In this case the course evaluation system provides you with a credential verifying that you completed the evaluation which contains your matriculation number. In this process the matriculation number is protected with cryptographic means and does not get known to the course evaluation system at any time.

CTI is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN), Munich, Germany, in setting up, running, and administering the University Registration System (data processor). For this it may become necessary to grant employees of NSN physical or online access to the University Registration System for administration purposes, validation of the system's functions as well as tracking and removing of errors. To protect the participant's personal data, precautions have been made. NSN employees may only access the system under the supervision of CTI staff. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by CTI employees in joint efforts with NSN. In this case, the personal data underlies the same security requirements as if they would reside with the university.

If you have any further questions about this project and your participation, you may contact Dr. Vasiliki Liagkou.

Please express your consent regarding the usage of your personal data in the pilot as described above by ticking the box below. You can revoke this consent at any time by contacting Dr. Vasiliki Liagkou who will then facilitate your withdrawal from the trial. Not consenting or revoking consent does not have negative implications on a participation in the university courses or the participation in the evaluation of lectures procured by CTI in parallel to this trial.

☐ By ticking this box, I indicate my willingness to voluntarily take part in the pilot. I have read and understood the terms and conditions and thereby agree that CTI processes my personal data. I agree that my matriculation number is processed and in case of winning a prize I agree to be identified on this basis.

Date: _____ Name: _____ Signature: _____

Please print your name

Please return the filled registration and consent forms to your lecturer or Dr. Vasiliki Liagkou.

Appendix B Pilot Information Sheet for the Participants

Computer Technology Institute and Press "Diophantus"

Vasiliki Liagkou

"D. Maritsas" Building, Nikou Kazantzaki street

University Campus of Patras

Rion, PO box 1382

265 00

email:Liagkou@cti.gr

Phone:2610960301 Fax:2610960490

Information sheet related to the pilot deploying Privacy-ABCs within the project ABC4Trust, round 2, winter semester 2013-2014

What is the ABC4Trust project?

The abbreviation "Privacy-ABCs" stands for "privacy enhancing Attribute-based Credentials". Privacy-ABC's are a technology that enables individuals preserving their privacy whenever they need to identify or register for an Information and Communication Technology (ICT) system. With the extensive distribution of systems requiring a secure authentication or identification of Users, in a broad range of scenarios, the Users' privacy is increasingly threatened. Privacy-ABCs allow the User to only reveal the information absolutely necessary for the execution of the required action and thus respect the privacy of the individual. Thus, Privacy-ABCs are a technological enabler for the privacy principle of **minimal disclosure**, making an anonymous or pseudonymous usage of many ICT services possible. The project ABC4Trust (Attribute Based Credentials for Trust)[8] is a research and development project funded by the European Union under its 7th Research Framework Program (FP7) as part of the ICT Trust & Security program. Having started in November 2010 with duration of four years, the project aims at achieving a more thorough understanding of Privacy-ABCs by enabling the deployment in practice and their federation in different domains.

The Student Pilot and participating as student

The ABC4Trust project launches a pilot deploying Privacy-ABCs at the Computer Technology Institute and Press "Diophantus" (CTI). The idea is to evaluate university lectures with the advantages of digital formats while preserving the anonymity and unlinkability of paper-based evaluation sheets. To allow unbiased feedback about the course and the person of the lecturer, the evaluation must be anonymous. To avoid that a single person evaluates the same lecture several times, or that persons have not registered for or participated in the lecture, an authentication towards the system is required. Using Privacy-ABCs, the information exchanged for this authentication will be strictly limited to the information necessary:

[8] See: https://abc4trust.eu/

- The student has registered for the particular course to be evaluated.
- The student has not yet given another evaluation for the same course. In case of multiple votes only the latest evaluation counts for the processing of the results.
- The student has attended a certain number of lectures to have a sufficient impression of the lecture.

It is not necessary for collecting and verifying class attendance or for participating in the evaluation that personal data of the students are processed.

Each participating student will receive a set of credentials matching the use case of the pilot. In this context, the term "credential" means a list of certified attributes inside a digital container. Proving these attributes will be necessary for the student to participate in a course evaluation. An example would be the proof that the owner of the credential is indeed student of the department offering the course, or that the student is registered to the course under evaluation and has attended a sufficient number of lectures. Credentials will be stored on a smart card provided by CTI. The credentials on the smart card are protected by the PIN known only to the participant.

Access to the obtained credentials is accomplished by a software component called "Client Application" that runs locally on User's machine. This software component is triggered every time a participant is required to provide data stored on her card. The client displays the policy of the service and the personal data that are requested to obtain the consent of the User prior to submitting the information. Moreover, it enables the student to browse, delete, or locally backup the Privacy-ABCs stored on the own smart card.

As a reward for participating in the pilot and for providing their feedback on the lecture, the students have the opportunity to take part in an optional tombola. For this the course evaluation system will issue an additional credential. To ensure the anonymity of the User's during the participation in the evaluation the class evaluation system must not learn the User's identity, and the feedback regarding the class must not be linkable to a specific student. Moreover, the tombola is only open for participants who have finished the evaluation, so their token should not be transferable to another User. To solve this dilemma, and to still allow the later identification of the winner, ABC4Trust deploys two advanced Privacy-ABCs features: Carry –over attributes and inspection. The course evaluation system issues a credential about the successful completion of the evaluation for the participant. The course evaluation system blindly inserts the students matriculation number obtained in encrypted format from the student into the tombola credential. It is cryptographically prevented that the course evaluation system obtains the clear-text value of the matriculation number enabling the identification of the participant (used feature: carry-over attributes). The student then provides a presentation token proving the participation in the evaluation. The token produced by the student's Client Application contains the own matriculation number encrypted to the secret key of a trusted third party, the inspector. From the collected presentation tokens, a winner is drawn. Only this token will be sent to the inspector for decrypting the matriculation number to notify the winner (used feature: inspection). Once the prize has been awarded the tombola tokens are deleted.

Further in-depth explanations and help regarding the handling of the smart card, the Client Application software, obtaining credentials or participating in the evaluation are given in the User manual available at the pilot's portal page:

https://ces.cti.gr/Portal/Portal.html

Treatment of personal data

For the registration process the following information will be collected by CTI from the students and processed in the university registration system for exclusive use within the pilot:

- First- and last name

- Matriculation number
- Name of the University (for this pilot: "University of Patras")
- Name of the department (for this pilot: "Department of Computer Engineering and Informatics")
- Courses the student is subscribed to (for the pilot: "Distributed Systems I")

During the evaluation phase, students will authenticate towards the course evaluation system using Privacy-ABCs. Students log in by only verifying that they are enrolled students of the university and have registered for the course in question. In addition, they need to prove a sufficient attendance in the lectures to evaluate. Students will then answer the questions of a questionnaire online. As the replies to these questions directly relate to the quality of a particular class, and directly or indirectly to teaching qualities of the lecturer, they entail personal data of the lecturer.

The named data is stored in the university registration system which is run and administered by CTI. The processing is necessary for the purpose of issuing the credentials or to re-issue credentials in case of lost smart cards. In addition, access to this data may become necessary for CTI to ensure and measure the functionality of the pilot system and for tracking and remove errors. Participants have the possibility to access and rectify data stored in the university registration system online, or by contacting CTI. Lecturers may access and see their personal data gathered by the system. Data such as the name of the lecturer and the title of the class may be rectified by notice to the data controller (CTI).

Issued credentials are stored on the smart card under the control of the participant and accessible only with the PIN which will be handed out to the participants.

The course evaluation system processes this information:

- Course/class (such as course "Distributed Systems I")
- Course attendance (counter collection for each visited course individually)
- Name of lecturer
- Survey answers (result course evaluation)
- Verification that attendance of the lecture is the minimum number or more

If the student wants to participate in the tombola the course evaluation system provides a credential verifying the participation and containing the matriculation number. In this process the course evaluation system does not see the matriculating number, but uses cryptographic mechanisms to copy it unknown to itself into the new credential.

CTI is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN), Munich, Germany, in setting up, running, and administering the university evaluation service. For this it may become necessary to grant employees of NSN physical or online access to the ABC system for administration purposes, validation of the system's functions as well as tracking and removing of errors. To protect the participant's personal data, precautions have been made. NSN can only access the system under the supervision of CTI. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by CTI employees or online. In this case, the personal data underlies the same security requirements as if it would reside with the university. Any communication between NSN and the ABC system will be protected against unauthorized access by third parties.

All personal information provided by the participants will be treated carefully and confidentially. It will be stored securely and will not be used or disclosed to third parties without the participant's

explicit consent. Since this pilot is part of scientific research project, aggregated and anonymized data will be used to complete the research work of this project as well as it will be used for academic purposes, like the publication of scientific proceedings; for drafting various informative reports, containing presentations of graphs and statistics that will be publicly available. The personal data collected, stored and processed will be deleted at latest 6 months after the end of the pilot.

Access to evaluation results by lecturers

To ensure the protection of the student participants, this right of access regarding the student's feedback is restricted during the evaluation period. This is to prevent that the information provided in a particular evaluation may be linked to an individual student. The lecturer is granted access to the cumulated results once the evaluation has finished. While chances for a successful attempt to identify a student submitting a particular evaluation are minimal, it might be possible if not enough students have submitted their evaluation. After the evaluation period, the lecturer may therefore view the individual feedback sheets of the evaluation, only if at least 5 students have provided feedback for the lecture (minimum anonymity set).

User consent, revoking consent, consequence of missing consent

The processing of personal data in this pilot falls under the scope of the Greek data protection law. To lawfully process this data, CTI needs an informed consent of each participant. Students are free to give consent and an already provided consent may be revoked any time by notice towards CTI. Not providing consent or revoking it later will not cause disadvantages in class. Please note that without giving consent, the student may not participate in the trial. The official evaluation of the class will nevertheless be possible, as the university department will procure the regular paper-based evaluation of the class for all attendees of the class regardless of participation in the trial.

Contact details of the data controller for questions and other inquiries::

Computer Technology Institute and Press "Diophantus"

"D. Maritsas" Building, Nikou Kazantzaki street

University Campus of Patras

Rion, 26500

Contact Person: Vasiliki Liagkou

0.1.10 Office on Zero floor of "D. maritsas" Building,

email:Liagkou@cti.gr

Tel:2610960301

More information about the project can be found at: www.abc4trust.eu

More information about the system is contained in the User manual to be found at: https://ces.cti.gr/Portal/Portal.html

Appendix C DPA (Data Protection Authority) notification

Computer Technology Institute and Press "Diophantus"

Vasiliki Liagkou

"D. Maritsas" Building, Nikou Kazantzaki street

University Campus of Patras

Rion, PO box 1382

265 00

email:Liagkou@cti.gr

Phone:2610960301 Fax:2610960490

Notification in accordance with Article 6 of Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data

Dear Madam, dear Sir,

the consortium of the European Commission-funded research and development project ABC4Trust notifies you about a personal data processing which will occur during a test trial of a system deploying Privacy-enhancing attribute-based credentials (Privacy-ABCs) system at the Computer Technology Institute and Press "Diophantus" department (CTI) at the university of Patras, Greece. In accordance with Article 6 of the Greek data protection law, we therefore provide information about the trial and the processing operations below as well as we may partially reference to annexed documents which are related.

Data controller:

Data controller is the Computer Technology Institute and Press "Diophantus" department (CTI) at the University of Patras, Greece. The address is stated above in the head of this letter. For any questions or inquiries about this notification, please refer to the contact information which is given at the end of this letter.

Location of established hardware supporting the data processing:

Personal data of students and lecturers at the CTI will be processed for an anonymous online course evaluation. For this, a Privacy-ABCs system was developed. All components are hosted under the control and responsibility of CTI in Patras, Greece. The students may use their own computer hardware at home to remotely access the provided online service.

Purpose of the data processing:

The ABC4Trust project partners are developing a technology Privacy-ABCs system that helps to protect the identity and privacy of Internet Users. Privacy-ABCs enable individuals to preserve their privacy whenever they need to authenticate or register for an Information and Communication Technology (ICT) system. Only the information absolutely necessary for the execution of the required action (minimal disclosure) needs to be disclosed.

Within this project, trials are conducted to obtain real User feedback on Privacy-ABCs systems and to learn how good the so far developed system works. The participants of the trial are students and lecturers at CTI who will be asked to give free and informed consent for the processing of their personal information (see consent forms in Appendix A). These trials will give the opportunity to test the usability and performance of the technology.

As the goal of the pilot is to verify and show the privacy-preserving features of Privacy-ABCs, some of the more advanced features need to be tested as well. To show this, a tombola will be opened for students who have participated in the evaluation, whereby the students are free to participate. To ensure the anonymity of the User's during the participation in the evaluation the class evaluation system must not learn the User's identity, and the feedback regarding the class must not be linkable to a specific student. Moreover, the tombola is only open for participants who have finished the evaluation, so their token should not be transferable to another User. To solve this dilemma and to still allow the later identification of the winner, ABC4Trust deploys two advanced Privacy-ABCs features: Carry–over attributes and inspection. The course evaluation system issues a credential about the successful completion of the evaluation for the participant. The course evaluation system blindly inserts the students matriculation number obtained in encrypted format from the student into the tombola credential. It is cryptographically prevented that the course evaluation system obtains the clear-text value of the matriculation number enabling the identification of the participant (used feature: carry-over attributes). The student then provides a presentation token proving the participation in the evaluation. The token produced by the student's Client Application contains the own matriculation number encrypted to the secret key of a trusted third party, the inspector. From the collected presentation tokens, a winner is drawn. Only this token will be sent to the inspector for decrypting the matriculation number to notify the winner (used feature: inspection). Once the prize has been awarded the tombola tokens are deleted.

For more in-depth information about Privacy-ABCs in this pilot trial, please look at the information sheet which is attached to this letter (Appendix B), or visit our website at

http://www.abc4trust.eu

Categories of personal data processed:

During the trial, the following personal data of students and lecturer of the concerned courses will be processed:

- Matriculation number of the student participants
- University (meaning the information that the participant is student/lecturer at CTI)
- Course/class (such as course "Distributed Systems I")
- Course attendance (counter on the smart card for the number of classes visited)
- Name of lecturer
- Results of the lecturer course evaluation
- Encrypted matriculation number of all tombola participants
- Clear-text Matriculation number and name of the student who was drawn as winner of the tombola

Time period of personal data processing and until data deletion:

The trial will be conducted from 24/9/2012 to 16/2/2012 (The second round of student pilot started at 15/10/2013--) The personal data which was processed during this trial will be deleted at latest 3 month after the end of the trail. Aggregated evaluation results will be stored and published based on consent of the lecturer. The correlating consent forms will be kept with CTI until 6 months after the end of the project and then deleted/destroyed (June 2015)

For academic purposes, like the publication of scientific proceedings, reports, or presentations trial results are used in anonymized and aggregated form only, e. g. as graphs and statistics made publicly available. The aggregated results may be used and published in project reports, scientific papers, presentations or other publications.

Recipients of personal data:

The CTI is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN) seated in Munich, Germany, in setting up, running, and administering a university course evaluation service. For these activities, it eventually may become necessary to grant employees of NSN physical or online access to the ABC system and log files for administration purposes, validation of the system's functions as well as tracking and removing of errors. The activities of NSN are governed by a processing contract (Annex 3)

To protect the participant's personal data, precautions have been made. NSN can only access the system under the supervision of CTI. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by CTI employees or online. In this case, the personal data underlies the same security requirements as if it would reside with the university. Any communication between NSN and the ABC system will be protected against unauthorized access by third parties, e. g. by encrypted communication.

Basic characteristics of the system and safety measures to protect the data:

The ABC4Trust project launches a pilot deploying Privacy-ABCs at the Computer Technology Institute and Press "Diophantus" (CTI). The idea is to enable an evaluation of university courses with the advantages of digital formats while preserving the anonymity and unlinkability of paper-based evaluation sheets. To allow unbiased feedback about the course and the person of the lecturer, the evaluation will be anonymous. To avoid that a single person evaluates the same lecture several times, or that persons have not registered for or participated in the lecture, an authentication towards the system is required. Using Privacy-ABCs, the information exchanged for this authentication will be limited to the information necessary and does not allow the identification of the User.

For a more in-depth information of the system that is set up and any technical and organizational measures to protect the personal data of the participants, we refer to the explanations and agreements which were made in the processing contract between CTI and NSN (Annex 3), as well as to existing research documents published by ABC4Trust at: https://abc4trust.eu/index.php/pub.

We hope that this notification including its annexed documents are sufficient to comply with the notification obligation as manifested in Article 6 of Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data. If this is not the case, or any other questions remain, please contact us using the contact details below.

We remain with best regards,

_____

Dr. Vasiliki Liagkou

Contact details of the data controller for questions and other inquiries::

Computer Technology Institute and Press "Diophantus"
"D. Maritsas" Building, Nikou Kazantzaki street
University Campus of Patras
Rion, 26500
Contact Person: Vasiliki Liagkou
0.1.10 Office on Zero floor of “D. maritsas” Building,
email:Liagkou@cti.gr
Tel:2610960301
More information about the project can be found at:
www.abc4trust.eu
More information about the system is contained in the User manual to be found at:
https://ces.cti.gr/Portal/Portal.html

Appendix D Student's Questionnaire

D.1 Student's Questionnaire for the First Round

Patras Pilot Evaluation

Questionnaire

D.1.1 Part 1: Privacy-ABCs evaluation

1. For the time of the trial different groups where formed to test the usage of the smart card. To evaluate the system in the following questionnaire we would first like to know if you did receive a smart card and if so for how long:

	yes	no
Did you receive a smart card?	☐	☐

In case of [no] please skip to question number 2.

	December 2012	January 2013
In which month did you receive the smart card?	☐	☐

	yes	no
Did you use the smart card for the course evaluation?	☐	☐

2. At the beginning of the trial you have been briefed about a technology called Privacy Attribute Based Credentials (or Privacy-ABCs for short) that was used during the pilot. The technology uses a smart card to collect credentials and course attendance data and offers then a privacy-enhanced way to authenticate to the Course Evaluation System (CES). Please mark the following statements as true or false according to your understanding of how this technology works:

	true	false	don't know
When I authenticate to the CES, the smart card transmits its unique serial number to the CES.	☐	☐	☐
When I authenticate to the CES, the smart card transmits the course identification number to the CES.	☐	☐	☐
When I authenticate to the CES, the smart card transmits the number of my class attendances to the CES.	☐	☐	☐
When I try to evaluate the same course for the second time, the CES knows that I have already done so, but it is still not able to identify me.	☐	☐	☐
When I access the CES from a PC, Privacy-ABCs anonymize my IP address.	☐	☐	☐
Imagine that you could evaluate two different courses in the CES. In this case the CES can tell that these two actions are done by the same person, even though it does not know by which one.	☐	☐	☐
If the police has valid reasons, the anonymity can be lifted and the person who did the evaluation can be identified.	☐	☐	☐

3. How strongly do you agree or disagree with the following statements? Please note that the Privacy-ABC-System includes all the ABC4trust User services (e.g., issuance of credentials, backup and restore of credentials, view of credentials, presentation of credentials), the smart card, and the smart card reader. It does not include the course evaluation system.

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
Learning to operate the Privacy-ABC-System would be easy for me.	☐	☐	☐	☐	☐
I would find it easy to make the Privacy-ABC-System to do what I want it to do.	☐	☐	☐	☐	☐
My interaction with the Privacy-ABC-System would be clear and understandable.	☐	☐	☐	☐	☐
I would find the Privacy-ABC-System to be flexible to interact with.	☐	☐	☐	☐	☐
It would be easy for me to become skillful at using the Privacy-ABC-System.	☐	☐	☐	☐	☐
I would find the Privacy-ABC-System easy to use.	☐	☐	☐	☐	☐

	never	once	some-times	often	don't know
4. Did you use the backup function of your smart card?	☐	☐	☐	☐	☐

	no, not at all				yes, very much
	1	2	3	4	5
5. Did you worry that you might lose your smart card?	☐	☐	☐	☐	☐

6. Do you have additional comments to the usage of the Privacy-ABC-System?

.....

.....

.....

.....

.....

.....

7. How strongly do you agree or disagree with the following statements?

	strongly disagree 1	2	neutral 3	4	strongly agree 5
Using Privacy-ABCs would give me control over my online privacy.	☐	☐	☐	☐	☐
Privacy-ABCs would be useful in protecting my online privacy.	☐	☐	☐	☐	☐
When using Privacy-ABCs, I would not always be able to effectively protect my online privacy.	☐	☐	☐	☐	☐
Despite Privacy-ABCs, a really determined attacker will be able to violate my online privacy.	☐	☐	☐	☐	☐
Using Privacy-ABCs would make it easier to protect my online privacy.	☐	☐	☐	☐	☐
Privacy-ABCs would prevent violation of my online privacy.	☐	☐	☐	☐	☐

8. Privacy-ABCs can provide anonymity for many Internet activities, including online payment. They can also hide your home address from the webshop if you buy something online. How useful would you find Privacy-ABCs in protecting your privacy in the following scenarios?

	every day	several times per week	several times per month	less often	never
Download content (such as music, movies, books, games, software)	☐	☐	☐	☐	☐
Access Social Media to look for updates, write posts, or upload photos or videos (e.g. forums, blogs, Facebook or other social networks, Twitter, Flickr, etc.)	☐	☐	☐	☐	☐
Make travel arrangements online (purchase a bus, train, or plane ticket, book a hotel, organize a holiday, etc.)	☐	☐	☐	☐	☐
Buy digital goods (such as music, movies, games, or programs from platforms like iTunes, Steam, Napster, or Amazon)	☐	☐	☐	☐	☐
Buy/sell physical goods (e.g. Ebay, eShop, etc.)	☐	☐	☐	☐	☐
Do online banking (check your balance, make a money transfer, etc.)	☐	☐	☐	☐	☐

9. Before you joined the trial for the Privacy-ABCs...

	yes	no	don't remember
have you ever used a paper-based course evaluation system in this or in some other university?	☐	☐	☐
have you ever used an electronic-based course evaluation system in this or in some other university?	☐	☐	☐

10. How strongly do you agree or disagree with the following statements? Please also answer the question if you never actually participated in some kinds of course evaluation.

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
It is important for me to protect my anonymity when participating in a course evaluation.	☐	☐	☐	☐	☐
I believe that the paper-based course evaluation system guarantees my anonymity.	☐	☐	☐	☐	☐
I believe that the paper-based course evaluation system is convenient to use.	☐	☐	☐	☐	☐
I believe that the Privacy-ABC-System-based course evaluation system guarantees my anonymity.	☐	☐	☐	☐	☐
I believe that the Privacy-ABC-System-based course evaluation system is convenient to use.	☐	☐	☐	☐	☐

11. Which form of course evaluation system would you prefer. Please check only one of the boxes below.

Paper-based	☐
Privacy-ABC-based	☐

12. How strongly do you agree or disagree with the following statements?

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
I trust that the Privacy-ABC-System does not reveal information about my identity because it contains technology developed by leading manufacturers.	☐	☐	☐	☐	☐
I trust that the Privacy-ABC-System does not reveal information about my identity because the environment of the system is controlled by University of Patras.	☐	☐	☐	☐	☐
I trust that the Privacy-ABC-System does not reveal information about my identity because the Privacy-ABC technology was built within the framework of an EU project.	☐	☐	☐	☐	☐
I trust that the Privacy-ABC-System does not reveal information about my identity because strong cryptographic algorithms are used.	☐	☐	☐	☐	☐

13. Assuming the Course Evaluation System (CES) including the Privacy-ABC-System will be permanently installed in the future, how strongly do you agree or disagree with the following statements?

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
I would not use the CES at all.	☐	☐	☐	☐	☐
I would use the CES without reservation.	☐	☐	☐	☐	☐
I would take time for learning how to use the CES.	☐	☐	☐	☐	☐

14. How strongly do you agree or disagree with the following statements?

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
Participating in course evaluations is important for me. ..	☐	☐	☐	☐	☐
Participation in course evaluations gives students more control over the quality of teaching.	☐	☐	☐	☐	☐
Results of course evaluations do not have much influence on the quality of teaching.	☐	☐	☐	☐	☐
Usually, I do not participate in course evaluations.	☐	☐	☐	☐	☐
Other students think that participating in the course evaluation is important.	☐	☐	☐	☐	☐
My friends usually participate in course evaluation.	☐	☐	☐	☐	☐

This concludes the first part and the questions about Privacy-ABC specific subjects. Thank you very much for your work so far. You have finished more than half of the questionnaire and now we would like to ask some more general questions:

D.1.2 Part 2: General privacy and demographic questions

15. How often do you do the following on the Internet? (choose the most appropriate answer)

	every day	several times per week	several times per month	less often	never
Download content (such as music, movies, books, games, software)	☐	☐	☐	☐	☐
Access Social Media to look for updates, write posts, or upload photos or videos (e.g. forums, blogs, Facebook or other social networks, Twitter, Flickr, etc.)	☐	☐	☐	☐	☐
Make travel arrangements online (purchase a bus, train, or plane ticket, book a hotel, organize a holiday, etc.)	☐	☐	☐	☐	☐
Buy digital goods (such as music, movies, games, or programs from platforms like iTunes, Steam, Napster, or Amazon)	☐	☐	☐	☐	☐
Buy/sell physical goods (e.g. Ebay, eShop, etc.)	☐	☐	☐	☐	☐
Do online banking (check your balance, make a money transfer, etc.)	☐	☐	☐	☐	☐

16. How strongly do you agree or disagree with the following statements?

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
Consumers have lost all control over how personal information is collected and used by companies.	☐	☐	☐	☐	☐
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	☐	☐	☐	☐	☐
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	☐	☐	☐	☐	☐

17. When you use the Internet services, such as search engines, online information portals, email, online social networks, online shops, how much are you worried about the following things:

	not worried				very worried
	1	2	3	4	5
Service providers might sell your personal data to some other companies.	☐	☐	☐	☐	☐
Your personal data might get stolen from the service providers.	☐	☐	☐	☐	☐
The government might monitor your activities.	☐	☐	☐	☐	☐
People you know personally (e.g. family members) might monitor your activities	☐	☐	☐	☐	☐

18. How much are you worried that the following types of your personal information might be available to businesses or people you don't know:

	not worried				very worried
	1	2	3	4	5
Your full name.	☐	☐	☐	☐	☐
Your date of birth.	☐	☐	☐	☐	☐
Your postal address.	☐	☐	☐	☐	☐
Your email-address.	☐	☐	☐	☐	☐
Your full bank account information.	☐	☐	☐	☐	☐
Your current location.	☐	☐	☐	☐	☐
Your hobbies.	☐	☐	☐	☐	☐
Your favorite meals.	☐	☐	☐	☐	☐

19. Please answer the following questions. If you never heard some term or are not sure what it means, please answer don't know.

	yes	no	don't know
Websites that I visit know the IP address of my computer.	☐	☐	☐
Cookies can collect personal information about a User from his or her computer.	☐	☐	☐
Cookies can be used in order to track people across different websites when they surf in the Internet.	☐	☐	☐
If people don't use their real names when writing in Internet forums, the police cannot find out their real names and addresses.	☐	☐	☐
Private browsing (also called private mode, privacy mode or incognito mode) guarantees that I can remain anonymous when surfing the Internet.	☐	☐	☐
If somebody knows my IP address, they usually can find out my approximate geographic location (e.g, part of the country, or the next big city.)	☐	☐	☐

20. Please answer the following questions. If you never heard some term or are not sure what it means, please answer don't know.

	yes	no	don't know
Do you sometimes clean cookies?	☐	☐	☐
Do you sometimes clean the browser history?	☐	☐	☐
Do you usually read the privacy policy of an online shop before buying anything there for the first time?	☐	☐	☐
Did you ever refrain from creating a web account or making an online purchase because of privacy concerns?	☐	☐	☐
Do you sometimes encrypt your emails?	☐	☐	☐
Do you sometimes use private mode in browsers? (also called privacy mode or incognito mode)	☐	☐	☐

21. How often did you experience the following problems?

	never	once	some-times	often	don't know
Fraudulent emails (phishing emails) constructed to steal your account information and/or your money.	☐	☐	☐	☐	☐
Unwanted photos or details about you published online. (e.g. party pictures on Flickr or Facebook)	☐	☐	☐	☐	☐
Credit card number theft (e.g. you entered payment information for a product or a service on a website that was faked solely to get that information from you)	☐	☐	☐	☐	☐
Virus or trojan infection on your computer.	☐	☐	☐	☐	☐

22. What is your year of birth? ..... 19 _ _

23. What is your gender? ..... Male ☐ Female ☐

D.2 Student's Questionnaire for the Second Round

Patras Pilot Evaluation

Questionnaire

Thank you for participating in our survey! Your support provides a crucial contribution to the success of the ABC4Trust project.

Your own opinion is most important, and therefore there are no right or wrong answers to the following questions. Please answer all questions conscientiously and completely. Take all the time you need to go through the questions and try to answer spontaneously and intuitively.

Please note that some of the questions may seem repetitive to you, but they are made so for more accurate measurements.

All information gathered will be used for academic purposes only and will be treated absolutely anonymously, ensuring that no one will be able to determine your identity based on the answers provided.

ABC4Trust Team
Contact Person: Vasia Liagkou

During the pilot you have the opportunity to test a technology called Privacy Attribute Based Credentials (or Privacy-ABCs for short). The technology uses a smart card to collect credentials and course attendance data and then enables you to participate in the evaluation of a course and in the Tombola lottery. We would like to know more about your usage of the Privacy- ABC technology and your opinion about it in order to improve the technology.

	yes	no
1. Did you receive the Privacy-ABC smart card at the beginning of the pilot? ...	☐	☐
If yes, did you use the smart card to get the university credentials?	☐	☐
Did you use the smart card to collect class attendances?	☐	☐

If you received a smart card, but did not use it for one of both of the above tasks, please write down the reasons: .....

.....

.....

.....

.....

.....

	yes	no
2. Did you evaluate the course using the online Course Evaluation System?	☐	☐

If not, please write down the reason: .....

.....

.....

.....

.....

	yes	no
3. Was Firefox your default browser before you started using Privacy-ABCs? ...	☐	☐

	very difficult				very easy
	1	2	3	4	5
Setting up Firefox for using Privacy-ABCs was:	☐	☐	☐	☐	☐

	yes	no
4. Did you use the backup function of your smart card?	☐	☐

If not, please write down the reason: .....

.....

.....

.....

.....

	very difficult				very easy
	1	2	3	4	5
If you used the backup function, the usage was:	☐	☐	☐	☐	☐

	no, not at all				yes, very much
	1	2	3	4	5
5. Did you worry that you might lose your smart card?	☐	☐	☐	☐	☐

	not comfortable at all				very comfortable
	1	2	3	4	5
6. How comfortable were you knowing that your personal data was saved on a smart card?	☐	☐	☐	☐	☐

	yes	no
7. Did you participate in the Tombola lottery?	☐	☐

If not, please write down the reason: .....

.....

.....

.....

.....

8. Please indicate your opinion about this statement (even if you did not participate in the Tombola):

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
I believe that the Inspector would not misuse his or her role for getting more information about the students.	☐	☐	☐	☐	☐

9. Which of the following possibilities for the Tombola Inspector do you prefer? Please answer even if you did not participate in the Tombola. Please check only ONE of the boxes below:

   I prefer a student to play the role of the Inspector. ..... ☐

   I prefer a member of CTI or University to play the role of the Inspector ..... ☐

   I don't care which of them plays the role of the Inspector ..... ☐

10. Please mark the following statements as "true", "false" or "don't know" according to your understanding of how this technology works:

	true	false	don't know
When I authenticate to the Course Evaluation System (called CES in the following), the smart card transmits my matriculation number to the CES.	☐	☐	☐
When I authenticate to the CES, the smart card transmits the number of my class attendances to the CES.	☐	☐	☐
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.	☐	☐	☐
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.	☐	☐	☐
When I access the CES from a PC, Privacy-ABCs anonymize my IP address.	☐	☐	☐

11. The pilot participants were able to obtain an additional credential, the Tombola credential, from the Course Evaluation System, after submitting their course evaluation. This credential proved that they participated in the evaluation and allowed them to access the Tombola system. Please mark the following statements as "true", "false" or "don't know" according to your under- standing of the Privacy-ABC technology. Please answer even if you did not participate in the tombola.

	true	false	don't know
Your tombola credential contains your matriculation number.	☐	☐	☐
The administrator of the Tombola system can decrypt your matriculation number if you are not the winner.	☐	☐	☐
The administrator of the Tombola system can decrypt the winner's matriculation number.	☐	☐	☐

12. Before you joined the trial for the Privacy-ABCs...

	yes	no
have you ever used a paper-based course evaluation system in this or in some other university?	☐	☐
have you ever used an electronic-based course evaluation system in this or in some other university?	☐	☐

13. Which form of course evaluation system would you prefer? Please check only ONE of the boxes: .....

Paper based	Privacy-ABCs based
☐	☐

14. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
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.	☐	☐	☐	☐	☐

15. The Privacy ABC system can provide anonymity in a lot of online scenarios. Would you like to use Privacy-ABCs for some online activities (other than course evaluation)? .....

yes	no
☐	☐

If yes, please name a few examples here:

.....

.....

.....

.....

.....

.....

.....

Please turn over to the next page

16. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree 1	2	neutral 3	4	strongly agree 5
My interaction with the Privacy-ABC system is clear and understandable.	☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
Obtaining a valid credential with the Privacy-ABC system is easy.	☐	☐	☐	☐	☐
I find it easy to manage (delete, restore, backup) my personal information on my smart card with the Privacy-ABCs.	☐	☐	☐	☐	☐
I found it easy to learn how to use the Privacy-ABC system.	☐	☐	☐	☐	☐
Often I could not remember how to interact with the Privacy-ABC system.	☐	☐	☐	☐	☐
Using the Privacy-ABC system takes too much time doing manual operations (for example clicks, data input, handling the smart card).	☐	☐	☐	☐	☐
The interface of the Privacy-ABC system is pleasant.	☐	☐	☐	☐	☐
I like using the interface of the Privacy-ABC system.	☐	☐	☐	☐	☐

17. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree 1	2	neutral 3	4	strongly agree
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.	☐	☐	☐	☐	☐
The Privacy-ABC system meets my requirements for a course evaluation.	☐	☐	☐	☐	☐
I find that the benefits of using the Privacy-ABC system are bigger than the effort to use it.	☐	☐	☐	☐	☐

18. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
The help information (such as on-line help, on-screen messages and other documentation) provided with the Privacy-ABC System is clear and understandable.	☐	☐	☐	☐	☐
It is easy to find the help information I need.	☐	☐	☐	☐	☐
The Privacy-ABC system provides very sensible and effective advice through the help information, if needed.	☐	☐	☐	☐	☐
The Privacy-ABC system provides competent guidance (as needed) through the help information.	☐	☐	☐	☐	☐
The Privacy-ABC system provides error messages that clearly tell me how to fix problems.	☐	☐	☐	☐	☐
Whenever I make a mistake using the Privacy-ABC system, I recover easily and quickly.	☐	☐	☐	☐	☐
The User Manual for the Privacy-ABC system is very helpful.	☐	☐	☐	☐	☐
CTI members as a support team of the Privacy ABC system provide whatever help I need related to the pilot.	☐	☐	☐	☐	☐

19. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
Participating in course evaluations is important to me. ...	☐	☐	☐	☐	☐
It is important to me to protect my anonymity when participating in course evaluations.	☐	☐	☐	☐	☐
I would see the decision to evaluate the course with the Privacy-ABC system as a risky action.	☐	☐	☐	☐	☐
The Privacy-ABC system is trustworthy.	☐	☐	☐	☐	☐

Please turn over to the next page

20. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree 1	2	neutral 3	4	strongly agree 5
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.	☐	☐	☐	☐	☐
The Privacy-ABC system is very reliable.	☐	☐	☐	☐	☐
The Privacy-ABC system has the functionality needed to protect my privacy.	☐	☐	☐	☐	☐
The Privacy-ABC system has the necessary features for protecting my privacy.	☐	☐	☐	☐	☐
The Privacy-ABC system has the ability to protect my privacy.	☐	☐	☐	☐	☐
The Privacy-ABC system does not malfunction.	☐	☐	☐	☐	☐
The Privacy-ABC system is extremely dependable.	☐	☐	☐	☐	☐

21. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree 1	2	neutral 3	4	strongly agree 5
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.	☐	☐	☐	☐	☐

22. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
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.	☐	☐	☐	☐	☐

You have finished more than 3/4 of the questionnaire! Thank you very much for your work so far. This concludes the questions about the Privacy-ABC system, and finally we would like to ask some more general questions.

23. Do you use the following Internet services?

	yes	no
Online banking	☐	☐
Online shopping	☐	☐
Social Networks (like Facebook, Google+, etc.)	☐	☐
Online storage (like photobucket, dropbox, etc.)	☐	☐

24. Please indicate how much you agree or disagree with the following statements. The range reaches from "strongly disagree" to "strongly agree".

	strongly disagree		neutral		strongly agree
	1	2	3	4	5
I am concerned that the information I submit on the Internet could be misused.	☐	☐	☐	☐	☐
When I shop on-line, I am concerned that the credit card or banking information can be stolen while being transferred on the Internet.	☐	☐	☐	☐	☐
I am concerned about submitting information on the Internet because of what others might do with it.	☐	☐	☐	☐	☐
I am concerned about submitting information on the Internet because it could be used in a way I did not foresee.	☐	☐	☐	☐	☐

25. Please indicate how often you do the following actions.

	Never		Sometimes		Very often
How often do you delete cookies from your computer?	☐	☐	☐	☐	☐
How often do you use private mode in browsers? (also called privacy mode or incognito mode)	☐	☐	☐	☐	☐
How often do you clean the browser history?	☐	☐	☐	☐	☐
When you enter your personal information on a Web site, how often do you read privacy policies?	☐	☐	☐	☐	☐
How often do you intentionally enter false information when creating a web account?	☐	☐	☐	☐	☐
How often do you decide not to create a web account or not to make an online purchase because of privacy concerns?	☐	☐	☐	☐	☐

.

26. Have you ever installed a privacy protection tool? (apart from Privacy-ABCs) Yes ☐ No ☐

If yes, please write down which privacy-protection tools you use or used before: .....
...

.....
...

.....
...

.....

27. What is your year of birth? ..... 19 __ ____

28. What is your gender? ..... male ☐ female ☐

This concludes the questionnaire. Thank you very much for your effort!

Appendix E Complementary Questionnaire

Please fill down your answer put it in the envelope and deliver it to Prof. Stamatiu's homework box at the university.

Question

Did you notice any differences when interacting with the ABC4Trust Pilot's systems by using your first (idemix) smart card and your second (U-Prove) smart card ?

Your Answer

-

Appendix F Patras Specification Document

F.1 Patras Pilot – 2ndRound - Pointers for Implementation

Basic idea: The pilot students register at the University and the pilot course by collecting the corresponding credentials from the University Registration System. The smart card creates a counter value associated to the course credential. The counter is kept in a trusted part of the smart card and is increased when attending the course lectures. For the course evaluation, the card will verify that the counter is above a certain threshold before participating in the course evaluation. The course evaluation will further check that the User has a university credential that is bound to the same key/smart card as the course credentials and that both credentials have not been revoked. When the student completes the evaluation she gets issued a new credential containing only her matriculation number which will be blindly carried over from the university credential. This new credential can be used for participating in an online tombola, where students that have participated in the online evaluation can win a special prize.

Differences to 1st-Round Pilot:

- support and integration of revocation of university/course credentials
- evaluation will check that student has two "valid" credentials (credCourse and credUniv)
- showing interoperability of UProve and Idemix, as all credUniv will be based on Idemix and all credCourse will be based on UProve (i.e. no seperation between Idemix and U-Prove cards anymore)
- using advanced issuance with carried-over attributes
- using the feature that a presentation policy can request for a particular pseudonym (Course Evaluation System)
- simplified backup/restore mechanism (backup of attendance data only)
- inspection

Use Cases:

1. Setup of all parameters
2. Registration & login of students
3. Obtaining the university & course credentials
4. Certification of class attendance
5. Participating in the evaluation
6. Participating in the tombola
7. Backup & Restore
8. Revocation
9. Inspection

Involved Parties:

- University Registration System (ABC Issuer & ABC Verifier)
- Class Attendance System
- Course Evaluation System (ABC Issuer & ABC Verifier)
- Revocation Authority (ABC Revocation Authority)
- Tombola System (ABC Verifier)
- Students (ABC User)
- Inspector (ABC Inspector)

F.2 Setup of all Parameters

The pilot administrator creates all parameters (cryptographic and non-cryptographic) needed in the course of the 2nd trial. In this context, the administrator initializes the pilot smart cards with the trusted parameters and triggers them to release a scope-exclusive pseudonym that will be used later on to identity eligible cards (resp. secret keys).

prerequisite: university maintains a list of all participating students
university has obtained non-initialized smart cards

Generate Privacy-ABC Parameters

- credential specification for university credential (credUniv), course credential (credCourse) and credTombola – please see appendix for xml credential specifications
- system parameters (trusted groups, generators for commitments, generators for pseudonyms etc)
- issuer parameters and issuer secret key for credUniv (issuerUniv), using Idemix settings
- issuer parameters and issuer secret key for credCourse (issuerCourse), using U-Prove settings
- issuer parameters and issuer secret key for credTombola (issuerTombola), using Idemix settings
- revocation authority parameters (key pair, system parameters, accumulator, revocation information)
- inspector parameters (key pair)

Generate Pilot Specific Parameters

- pk_root, sk_root for the root of the "pilot PKI"

- signature keys pk_cas, sk_cas for the authentication of the Class Attendance System
- one-time-passwords (OTP) for all students and keep a list of OTP_i associated to matriculation number of student_i

Initialize, Register & Distribute the smart cards

- Set the card to “root” mode
- Set the card's authentication key “0” with the value of pk_root (“SET AUTHENTICATION KEY” command)
- call smart card command “INITIALIZE DEVICE” with a chosen device identifier and decrypt the PIN/PUK values with sk_root (this procedure also triggers the generation of the device key)
- set the algebraic group “0” (modulus, group order, cofactor, generator) for device public key and pseudonyms (“SET GROUP COMPONENT” command)
- set the algebraic group “1” for issuerUniv (“SET GROUP COMPONENT” command)
- set the algebraic group “2” for issuerCourse (“SET GROUP COMPONENT” command)
- set the algebraic group “3” for issuerTombola (“SET GROUP COMPONENT” command)
- set the card's authentication key “1” with the value of pk_cas (“SET AUTHENTICATION KEY” command)
- create a counter with a minimum attendance threshold associated with the pk_cas (“SET COUNTER” command)
- create credUniv issuer associated to the previously defined algebraic group (“SET ISSUER” command)
- create credCourse issuer associated with the corresponding algebraic group and the previously defined counter (“SET ISSUER” command)
- create credTombola issuer associated with the corresponding algebraic group (“SET ISSUER” command)
- create a prover where the university credential can be mixed with pseudonyms during proof sessions (“SET PROVER” command)
- create a prover for the course credential (“SET PROVER” command)
- create a prover for the tombola credential (“SET PROVER” command)
- set the smart card to working mode (“SET WORKING MODE” command)
- invoke the card to obtain a scope-exclusive pseudonym for the scope "urn:patras:registration" and store the returned pseudonym on a list of trusted devices
- for each card, store deviceID, the scope-exclusive pseudonym, and a flag marking the card as "unregistered"
- distribute smart cards, together with one-time-passwords, PIN & PUK to students
- publish all public parameters, signed with sk_root and keep secret parts of the generated parameters in trusted storage

F.3 Registration & Login of Students

Registration

When a student logs in to the university registration system for the first time, she has to register her smart card, such that the university registration system can link the smart card (and associated personal data) to the matriculation number/student record. To this end, the student and the smart card must both authenticate towards the university registration system.

prerequisite: students have received their smart cards, OTP, PIN & PUK

university has a list of valid smart card pseudonyms and links between OTP & matriculation number

- student logs in at the university system and authenticates via matriculation number and OTP
- if authentication is successful (i.e. entry of matriculation number/OTP exist in university records) the university sends a presentation policy that requests to authenticate with a scope-exclusive pseudonym using the same scope ("urn:patras:registration") as in the setup.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!-- This is a sample ABC4Trust presentation policy for... -->

<abc:PresentationPolicyAlternatives xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0" Version="1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 ../../../../../../../../../
    abc4trust-xml/src/main/resources/xsd/schema.xsd">
  <abc:PresentationPolicy PolicyUID="urn:patras:policies:loginPseudonym">
    <abc:Message>
      <abc:Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</abc:Nonce>
    </abc:Message>
    <abc:Pseudonym Exclusive="true" Scope="urn:patras:registration"/>
  </abc:PresentationPolicy>
</abc:PresentationPolicyAlternatives>
```

Figure 42: Presentation Policy for Registration at the University Registration System

- the student invokes the UserABCE.createPresentationToken()method with the received presentation policy to obtain the presentation token containing the requested pseudonym. The generation of the presentation token requires presence of the student's smart card.
- the university verifies the token by calling the VerifierABCE.verifyTokenAgainstPolicy() method of the ABCE.
- The university registration system will recover the pseudonym value of the scope-exclusive pseudonym in the returned presentation token description. The system will check that the pseudonym value is among the ones generated during the setup phase and is marked as "unregistered".
- if verification is successful, the university system associates the pseudonym with the matriculation number and marks the pseudonym as "registered"

Login

For any subsequent login of the student to the university system, the student can authenticate directly using Privacy-ABC technologies. To this end, the university and student run the protocol above, starting with the exchange of the presentation policy loginPseudonym.

F.4 Obtaining the University & Course Credentials

When the student is logged in at the university registration system she can obtain a university credential certifying personal attributes and her student status (credUniv), as well as a course credential certifying her registration at the pilot course (credCourse).

prerequisite: student is already registered and logged in at the university registration system.

Obtaining CredUniv

- the student sends a credential request for urn:patras:credspec:credUniv
- the university registration system responds with an issuance message which contains the issuance policy that specifies that the newly issued credential will be bound to the same secret key as the (scope-exclusive) pseudonym that the User has already established. To this end, it invokes the IssuerABCE.initIssuanceProtocol()method on input the issuance policy stated below and the known attributes of the student.

Note: Neither the ABCE nor the presentation policy support a request & check yet that a presented pseudonym in the issuance token is a particular pseudonym, e.g., from another presentation token. In the pilot, this check must be done by the university system itself, in order to ensure that a credential is bound to the same student/card that is logged in.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!-- This is the issuance policy for issuance of the PATRAS University credential. -->

<abc:IssuancePolicy Version="1.0" xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 ../../../../../../../../
    abc4trust-xml/src/main/resources/xsd/schema.xsd">
  <abc:PresentationPolicy PolicyUID="urn:patras:policies:issuance:credUniv:revocable">
    <abc:Pseudonym Exclusive="true" Scope="urn:patras:registration" Established="false" Alias="#nym"/>
  </abc:PresentationPolicy>
  <abc:CredentialTemplate SameKeyBindingAs="#nym">
    <abc:CredentialSpecUID>urn:patras:credspec:credUniv:revocable</abc:CredentialSpecUID>
    <abc:IssuerParametersUID>urn:patras:issuer:idemix</abc:IssuerParametersUID>
  </abc:CredentialTemplate>
</abc:IssuancePolicy>
```

Figure 43: Issuance Policy for the University Credential

- the student and university registration system subsequently run the issuance protocol by calling the issuanceProtocolStep()method on their local ABCE, until the methods indicate completion of the protocol.

- During credUniv issuance the University Registration System contacts the Revocation Authority in order to obtain a revocation handle. The Revocation Authority replies with the next revocation handle and a witness. The revocation handle is stored in the IDM database and is associated with the specific student.

Obtaining CredCourse

- the student sends a credential request for urn:patras:credspec:credCourse

- the university registration system responds with an issuance message which contains the issuance policy that specifies that the newly issued credential will be bound to the same secret key as the scope-exclusive pseudonym that the User has already established. To this end, it invokes the IssuerABCE.initIssuanceProtocol()method on input the issuance policy stated below and passes the received issuance message to the User.

Note: Neither the ABCE nor the presentation policy support a request & check yet that a presented pseudonym in the issuance token is a particular pseudonym, e.g., from another presentation token. In the pilot, this check must be done by the university system itself, in order to ensure that a credential is bound to the same student/card that is logged in.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!-- This is the issuance policy for issuance of the Patras course credential. -->

<abc:IssuancePolicy Version="1.0" xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 ../../../../../../../../
    abc4trust-xml/src/main/resources/xsd/schema.xsd">
  <abc:PresentationPolicy PolicyUID="urn:patras:policies:issuance:credCourse">
    <abc:Pseudonym Exclusive="true" Scope="urn:patras:registration" Established="true" Alias="#nym"/>
  </abc:PresentationPolicy>
  <abc:CredentialTemplate SameKeyBindingAs="#nym">
    <abc:CredentialSpecUID>urn:patras:credspec:credCourse</abc:CredentialSpecUID>
    <abc:IssuerParametersUID>urn:patras:issuer:uprove</abc:IssuerParametersUID>
  </abc:CredentialTemplate>
</abc:IssuancePolicy>
```

Figure 44: Issuance Policy for the Course Credential

- the student and university registration system subsequently run the issuance protocol by calling the issuanceProtocolStep()method on their local ABCE, until the methods indicate completion of the protocol.

F.5 Certifying Class Attendance

When a student attends a course lecture, she is eligible to obtain a certification of that attendance. This certification must not be clone-able and the student should remain anonymous and un-linkable when obtaining the certification.

prerequisite: the student's smart card has been initialized with a counter associated with the public key of the class attendance system

The certification is done by increasing a counter in the trusted part of the smart card. Thereby, the counter can be increased only i) once per lecture, ii) when triggered by a legitimate class attendance system.

Offline setup

Before the lecture, the pilot administrator setups the CAS with a fresh lectureID (which must be strictly increasing, for each new lecture). This lecture ID could for example be equal to the current date (encoded as an integer), or simply be 1 for the first lecture, 2 for the second, and so on (set lectureID = newcursor).

Protocol

In order to certify the attendance at the lecture, the smart card (SC) and the class attendance system (CAS) run the following protocol:

- The SC generates a random nonce challenge. It sends the nonce to the CAS and also stores it locally (“GET CHALLENGE(16) command – returns a 16 byte fresh challenge).

- Upon receiving the random challenge, the CAS produces the following signature sig (based on the signature algorithm described on the Appendix of smart card manual) :

  - sig = Sign(sk_cas, counterId || newcursor || challenge).

- The SC attempts to increase by one the counter identified by counterId, verifying the signature sig with the public key of the class attendance system (“INCREMENT COUNTER(counterID, sig)” command):

  - Verify(pk_cas, sig, m) = true for m = counterID || newcursor || challenge, i.e. it verifies the signature against the stored public key and for the message including the nonce challenge that was generated by the SC in previous step.
  - cursor < newcursor, i.e. it sees a fresh lectureID

If one of the checks fails, or no counter blob for courseID was stored, it indicates failure towards the card reader. Otherwise, the SC increments the counter value by one, sets cursor = newcursor and indicates successful counter update towards the CAS.

F.6 Participating in the Course Evaluation

At the end of each semester the students that are enrolled in a course and have attended sufficiently many lectures are allowed to evaluate the quality of the course via the online course evaluation system. It must be ensured that only eligible students can participate but at the same time the students must remain anonymous towards the course evaluation system.

Evaluating the Course

prerequisite: the student has obtained credUniv and credCourse credentials and has attended sufficient course lectures.

- The Course Evaluation System ABCE as well as the User (student) ABCE obtain the latest revocation information from the Revocation Authority. On the User side this is done within the ABCE during the generation of the presentation token.
- When the student wants to evaluate a course, the course evaluation system sends the presentation policy urn:patras:policies:courseEvaluation which is depicted below. This policy requires the student to present a scope-exclusive pseudonym for the scope urn:patras:evaluation, in order to ensure that each student can create only a single pseudonym for this purpose (and thus evaluate the course once). The student has further to prove possession of a non-revoked university credential as well as a course credential for the course under evaluation. Finally, it is required from the student to prove that the university credential, the course credential and the pseudonym belong to the same secret key.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!-- This is a sample ABC4Trust presentation policy for... -->

<abc:PresentationPolicyAlternatives xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0" Version="1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 ../../../../../../../../../
    abc4trust-xml/src/main/resources/xsd/schema.xsd">
  <abc:PresentationPolicy PolicyUID="urn:patras:policies:courseEvaluation">
    <abc:Message>
      <abc:Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</abc:Nonce>
    </abc:Message>
    <abc:Pseudonym Exclusive="true" Scope="urn:patras:evaluation" SameKeyBindingAs="#credCourse"/>
    <abc:Credential Alias="#credCourse">
      <abc:CredentialSpecAlternatives>
        <abc:CredentialSpecUID>urn:patras:credspec:credCourse</abc:CredentialSpecUID>
      </abc:CredentialSpecAlternatives>
      <abc:IssuerAlternatives>
        <abc:IssuerParametersUID>urn:patras:issuer:uprove</abc:IssuerParametersUID>
      </abc:IssuerAlternatives>
    </abc:Credential>
    <abc:Credential Alias="#credUniv" SameKeyBindingAs="#credCourse">
      <abc:CredentialSpecAlternatives>
        <abc:CredentialSpecUID>urn:patras:credspec:credUniv:revocable</abc:CredentialSpecUID>
      </abc:CredentialSpecAlternatives>
      <abc:IssuerAlternatives>
        <abc:IssuerParametersUID>urn:patras:issuer:idemix</abc:IssuerParametersUID>
      </abc:IssuerAlternatives>
    </abc:Credential>
    </abc:PresentationPolicy>
 </abc:PresentationPolicyAlternatives>
```

Figure 45: Presentation Policy of the Course Evaluation System

- the student invokes the UserABCE.createPresentationToken() method with the received presentation policy to obtain the presentation token containing the requested information. The generation of the presentation token requires presence of the student's smart card.
- when the smart card recognizes that it should participate in the generation of a presentation token related to credCourse, it checks if the counter value of the associated counter blob exceeds the threshold that is contained in the counter blob as well. Only if this check succeeds, the smart card will proceed with the generation of its part of the presentation token, and indicate failure otherwise.
- upon receiving the presentation token the course evaluation system calls VerifierABCE.verifyTokenAgainstPolicy()on input the token and the policy. If the method returns a PresentationTokenDescription to indicate that the token fulfils the policy, the course evaluation system extracts the pseudonym value and checks whether an evaluation was already done under that pseudonym. In case it sees a fresh pseudonym, it finally allows the student to participate in the poll and stores the pseudonym.
- if the pseudonym was already used, either abort or allow to re-evaluate and thereby invalidate the previous evaluation (requires to keep track of all evaluations & pseudonyms)

Obtaining credTombola

prerequisite: the student has submitted the course evaluation

As soon as a student has submitted her course evaluation, she gets issued a credTombola credential that permits her to participate in an online tombola and have the chance to win a prize. The credTombola credential should contain the student's matriculation number which will later be used for participating in the tombola. Note that the Course Evaluation System never learns the student's matriculation number as we use an advanced issuance protocol with carry-over attribute. More precisely, the matriculation number is "blindly" carried over from the student's credUniv to the credTombola credential. Moreover, the presentation policy requests from the student to present that she possesses the scope exclusive pseudonym for scope "urn:patras:evaluation", that she has logged-in with at the Course Evaluation System.

- the student sends a credential request for urn:patras:credspec:credTombola
- the course evaluation system responds with an issuance message which contains the issuance policy that specifies that the newly issued credential will "blindly" carry over the matriculation number from credUniv, which is bound to the same key as the scope-exclusive pseudonym the student used for the evaluation. To this end, it invokes the IssuerABCE.initIssuanceProtocol()method on input the issuance policy stated below and passes the received issuance message to the User.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!-- This is the issuance policy for issuance of the PATRAS Tombola credential. -->

<abc:IssuancePolicy xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0" Version="1.0">
  <abc:PresentationPolicy PolicyUID="urn:patras:policies:issuance:credTombola">
    <abc:Message>
      <abc:FriendlyPolicyName lang="en">Issuance of Tombola Credential</abc:FriendlyPolicyName>
      <abc:FriendlyPolicyDescription lang="en">This policy will blindly carry over the matriculation
      number for user's credUniv to the credTombola credential</abc:FriendlyPolicyDescription>
    </abc:Message>
    <abc:Pseudonym Exclusive="true" Scope="urn:patras:evaluation" Alias="#nym">
          <abc:PseudonymValue>UDHlYk3VOuN5nYCnllUnguUINXOYdrxmUCvO/1QNARNbDpv/9KC3fRNbvX7i9PcpM38
          T0sTvjzDAyUrtm28AZsRIfQxyfqH7HI0+JA==</abc:PseudonymValue>
    </abc:Pseudonym>
    <abc:Credential Alias="#credUniv" SameKeyBindingAs="#nym">
      <abc:CredentialSpecAlternatives>
        <abc:CredentialSpecUID>urn:patras:credspec:credUniv</abc:CredentialSpecUID>
      </abc:CredentialSpecAlternatives>
      <abc:IssuerAlternatives>
        <abc:IssuerParametersUID>urn:patras:issuer:idemix</abc:IssuerParametersUID>
      </abc:IssuerAlternatives>
    </abc:Credential>
  </abc:PresentationPolicy>
  <abc:CredentialTemplate>
    <abc:CredentialSpecUID>urn:patras:credspec:credTombola</abc:CredentialSpecUID>
    <abc:IssuerParametersUID>urn:patras:issuer:idemix</abc:IssuerParametersUID>
     <abc:UnknownAttributes>
      <abc:CarriedOverAttribute TargetAttributeType="urn:patras:credspec:credTombola:matriculationnr">
        <abc:SourceCredentialInfo Alias="#credUniv" AttributeType="urn:patras:credspec:credUniv:matriculationnr"/>
      </abc:CarriedOverAttribute>
    </abc:UnknownAttributes>
  </abc:CredentialTemplate>
</abc:IssuancePolicy>
```

Figure 46: Issuance Policy of the Tombola Credential

• the student and the course evaluation system subsequently run the issuance protocol by calling the issuanceProtocolStep()method on their local ABCE, until the methods indicate completion of the protocol.

F.7 Participating in the Tombola

When the course evaluation period is over, the students can use the credTombola credential they got issued from the Course Evaluation System and participate in an on-line tombola that raffles a special prize.

prerequisite: the student has submitted the course evaluation and has obtained the credTombola credential from the Course Evaluation System.

• When the student wants to participate in the tombola, the tombola system sends the presentation policy urn:patras:policies:Tombola which is depicted below. This policy requests from the student to present a scope exclusive pseudonym for the scope “urn:patras:tombola”, to prove possession of a non-

revoked credUniv and to verifiably encrypt her matriculation number from credTombola with the Inspector's public key.

```
<abc:PresentationPolicyAlternatives xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"  Version="1.0">
<abc:PresentationPolicy PolicyUID="urn:patras:policies:Tombola">
    <abc:Message>
        <abc:Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</abc:Nonce>
        <abc:FriendlyPolicyName lang="en">Patricipating in the Tombola</abc:FriendlyPolicyName>
        <abc:FriendlyPolicyDescription lang="en">This policy requests from the student to present a
        scope exclusive pseudonym for the scope "urn:patras:tombola", to prove possession of a non-revoked
        credUniv and to verifiably encrypt her matriculation number with the Inspector's public key.
        </abc:FriendlyPolicyDescription>
    </abc:Message>
<abc:Pseudonym Exclusive="true" Scope="urn:patras:tombola" SameKeyBindingAs="#credTombola" />
<abc:Credential SameKeyBindingAs= "#credTombola">
      <abc:CredentialSpecAlternatives>
        <abc:CredentialSpecUID>urn:patras:credspec:credUniv</abc:CredentialSpecUID>
      </abc:CredentialSpecAlternatives>
      <abc:IssuerAlternatives>
        <abc:IssuerParametersUID>urn:patras:issuer:credUniv:idemix</abc:IssuerParametersUID>
      </abc:IssuerAlternatives>
    </abc:Credential>
<abc:Credential >
      <abc:CredentialSpecAlternatives>
        <abc:CredentialSpecUID>urn:patras:credspec:credTombola</abc:CredentialSpecUID>
      </abc:CredentialSpecAlternatives>
      <abc:IssuerAlternatives>
        <abc:IssuerParametersUID>urn:patras:issuer:credTombola:idemix</abc:IssuerParametersUID>
      </abc:IssuerAlternatives>
<abc:DisclosedAttribute AttributeType="urn:patras:credspec:credTombola:matriculationnr">
        <abc:InspectorAlternatives>
          <abc:InspectorPublicKeyUID>urn:patras:inspectorpk</abc:InspectorPublicKeyUID>
        </abc:InspectorAlternatives>
        <abc:InspectionGrounds>
          When the tombola is over, the Inspector can decrypt the matriculation number of the
          winner presentation token.
        </abc:InspectionGrounds>
      </abc:DisclosedAttribute>
    </abc:Credential>
  </abc:PresentationPolicy>
</abc:PresentationPolicyAlternatives>
```

Figure 47: Presentation Policy of the Tombola System

- the student invokes the UserABCE.createPresentationToken() method with the received presentation policy to obtain the presentation token containing the requested information. The generation of the presentation token requires presence of the student's smart card.
- upon receiving the presentation token the tombola system calls VerifierABCE.verifyTokenAgainstPolicy() on input the token and the policy. If the method returns a PresentationTokenDescription to indicate that the token fulfils the policy, the tombola system stores the student's scope-exclusive pseudonym along with the presentation token in its database.
- The Tombola System must ensure that there is a single entry in the database for specific scope-exclusive pseudonyms in order to prevent students from trying to register multiple times for the raffle.

• When the tombola is over, the Tombola System picks a random pseudonym and the corresponding presentation token from its database and contacts the Inspector in order to reveal the matriculation number of the winner.

F.8 Backup & Restore

The students should be able to back-up their smart card contents (device specific data, attendance data) in a way such that in case the original smart card get lost or broken, the data can be restored on a new, legitimate card, without harming the "uncloneability" of the data.

To allow for backup & restore, all cards are equipped with a master backup key stored on trusted storage.

Backup

prerequisite: the student has installed the User Application on her PC and has obtained a smart card

The User starts her User Application and clicks on backup button. Then she is asked to enter her PIN as well as a password that is required for restoring the backup file. An encrypted archive of her smart card data (device data and key, counters) is stored locally on her PC.

The smart card provides 3 mechanisms that are required for the backup procedure:

• a mechanism that backups device specific data (deviceID, PIN, PUK and device private key). This mechanism (“BACKUP DEVICE” command) requires from the User to enter the card PIN as well as a password that is required for restoring the values. In case, the correct PIN is entered a secure archive with the data blob “PIN || PUK || deviceKey” is stored locally.

• a mechanism that backups counter specific data (counter id, index and cursor). This mechanism (“BACKUP COUNTERS” command) requires from the User to enter the card PIN as well as a password required for restoring the values. If the User enters a correct PIN a secure archive with the data blob “counterID || index || cursor” is stored locally.

• a mechanism that backups credentials one by one. This mechanism (“BACKUP CREDENTIAL” command) requires from the User to enter the card PIN as well as a password and the credential id. If the User enters a correct PIN a secure archive with the data blob “credentialID || issuerID || status || prescounte || u” is stored locally.

Since revocation will be in place for the second round, the User Application needs to back-up only the attendance counter value. There is no need to backup credUniv and credCourse credentials since we can revoke the old ones (e.g. when a student loses her smart card) and issue fresh credentials to the new card.

Restore

prerequisite: the student has installed the User Application on her PC, has a back-up file of her attendance data and has obtained a new smart card with the same identifier from the pilot administrators

When a student needs to obtain a new smart card, due to the loss or malfunction of the original one, she can contact a university representative of the pilot with a valid identification document. Before providing the new smart card, the pilot administrator should revoke the student's credentials and delete her scope exclusive pseudonym from the University Registration System database.

The new smart card must be initialized by the university representative with the same device identifier as that of the previous card. The new PIN and PUK values are provided to the student along with the smart card.

When the User obtains her new card she can trigger the User Application and do the following procedure. She clicks on the restore button and selects the archive from her PC to restore on the card. She is asked to enter the new PIN and the password that is associated with the backup archive. If the deviceID is the same as before the restore takes place and the User now has in her new card the old data (PIN, PUK, deviceKey and counters).

The smart card provides 3 mechanisms that are required for the restore procedure:

- a mechanism that restores device specific data (deviceID, PIN, PUK and device private key). This mechanism ("RESTORE DEVICE" command) requires from the User to enter the card PIN as well as the password that was used for backup.

- a mechanism that restores counter specific data (counter id, index and cursor). This mechanism ("RESTORE COUNTERS" command) requires from the User to enter the card PIN as well as the password that was used for backup.

- a mechanism that restores credentials. This mechanism ("RESTORE CREDENTIAL" command) requires from the User to enter the card PIN as well as the password that was used for backup.

It is important that the restoration of a smart card is only allowed before the course evaluation period has started, in order to avoid students evaluating the course multiple times.

F.9 Revocation

In certain cases e.g. when a student leaves the university or when a smart card is stolen, the pilot administrators will need to revoke the student university and course credential in order to prevent "unauthorized" participation in the course evaluation.

When an administrator wants to revoke a credUniv or a credCourse, she browses the IDM database and finds the revocation handle for that credential. Then, using the University Registration System

administrator GUI she requests from the Revocation Authority to revoke this handle. The Revocation Authority revokes this handle and updates the revocation information.

When a pilot administrator revokes a credUniv or credCourse, she should also delete the student scope exclusive pseudonym for scope “urn:patras:registration” from the IDM database. This measure is needed in certain cases, e.g. when a smart card with the PIN on it, is stolen, in order to prevent “unauthorized” Users to browse the personal attributes of the original card holder.

F.10 Inspection

When the tombola is over and the winning presentation token has been selected, the pilot administrator contacts the Inspector. The Inspector can decrypt the matriculation number from the presentation token and the student who has won is announced.

F.11 Appendix

In this section we describe the credential specifications, for the credentials that will be used in the 2nd round of Patras pilot.

Credential Specification CredUniv

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
    This is credential specification for the PATRAS University credential.
-->
<abc:CredentialSpecification xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"
Version="Version 1.0" KeyBinding="true" Revocable="true">
  <abc:SpecificationUID>urn:patras:credspec:credUniv:revocable</abc:SpecificationUID>
  <abc:FriendlyCredentialName lang="en">Revocable University Credential</abc:FriendlyCredentialName>
  <abc:DefaultImageReference>https://idm.cti.gr/...</abc:DefaultImageReference>
  <abc:AttributeDescriptions MaxLength="256">
    <abc:AttributeDescription Type="http://abc4trust.eu/wp2/abcschemav1.0/revocationhandle"
    DataType="xs:integer" Encoding="urn:abc4trust:1.0:encoding:integer:unsigned"/>
    <abc:AttributeDescription Type="urn:patras:credspec:credUniv:firstname" DataType="xs:string"
    Encoding="urn:abc4trust:1.0:encoding:string:sha-256">
      <abc:FriendlyAttributeName lang="en">first name</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
    <abc:AttributeDescription Type="urn:patras:credspec:credUniv:lastname" DataType="xs:string"
    Encoding="urn:abc4trust:1.0:encoding:string:sha-256">
      <abc:FriendlyAttributeName lang="en">last name</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
    <abc:AttributeDescription Type="urn:patras:credspec:credUniv:university" DataType="xs:string"
    Encoding="urn:abc4trust:1.0:encoding:string:sha-256">
      <abc:FriendlyAttributeName lang="en">university name</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
    <abc:AttributeDescription Type="urn:patras:credspec:credUniv:department" DataType="xs:string"
    Encoding="urn:abc4trust:1.0:encoding:string:sha-256">
      <abc:FriendlyAttributeName lang="en">department name</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
    <abc:AttributeDescription Type="urn:patras:credspec:credUniv:matriculationnr" DataType="xs:integer"
    Encoding="urn:abc4trust:1.0:encoding:integer:unsigned">
      <abc:FriendlyAttributeName lang="en">matriculation number</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
  </abc:AttributeDescriptions>
</abc:CredentialSpecification>
```

Figure 48: University Credential Specification

Credential Specification CredCourse

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!--
    This is credential specification for the PATRAS course credential.
-->
<abc:CredentialSpecification xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"
Version="Version 1.0" KeyBinding="true" Revocable="false">
  <abc:SpecificationUID>urn:patras:credspec:credCourse</abc:SpecificationUID>
  <abc:FriendlyCredentialName lang="en">Course Credential</abc:FriendlyCredentialName>
  <abc:DefaultImageReference>https://idm.cti.gr/... </abc:DefaultImageReference>
  <abc:AttributeDescriptions MaxLength="256">
    <abc:AttributeDescription Type="urn:patras:credspec:credCourse:courseid"
    DataType="xs:string" Encoding="urn:abc4trust:1.0:encoding:string:sha-256">
      <abc:FriendlyAttributeName lang="en">course id</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
  </abc:AttributeDescriptions>
</abc:CredentialSpecification>
```

Figure 49: Course Credential Specification

Credential Specification CredTombola

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!--
    This is credential specification for the PATRAS Tombola credential.
-->
<abc:CredentialSpecification xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"
Version="Version 1.0" KeyBinding="false" Revocable="false">
  <abc:SpecificationUID>urn:patras:credspec:credTombola</abc:SpecificationUID>
  <abc:FriendlyCredentialName lang="en">Tombola Credential</abc:FriendlyCredentialName>
  <abc:DefaultImageReference>https://idm.cti.gr/...</abc:DefaultImageReference>
  <abc:AttributeDescriptions MaxLength="256">
    <abc:AttributeDescription Type="urn:patras:credspec:credTombola:matriculationnr"
    DataType="xs:integer" Encoding="urn:abc4trust:1.0:encoding:integer:unsigned">
      <abc:FriendlyAttributeName lang="en">matriculation number</abc:FriendlyAttributeName>
    </abc:AttributeDescription>
  </abc:AttributeDescriptions>
</abc:CredentialSpecification>
```

Figure 50: Tombola Credential Specification

List of Acronyms

ABCs	Attribute Based Credentials
Privacy-ABCs	Privacy Attribute Based Credentials (privacy ABCs)
ABCE	ABC Engine
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (HTTP secured by TLS or SSL)
HQAA	Hellenic Quality Assurance Agency
ID	Identifier
Idemix	IBM Identity Mixer
IdM	Identity Management System
NFC	Near Field Communication
PC	Personal Computer
PIN	Personal Identification Number
PUK	Personal Unblocking Key
PrimeLife	Privacy and Identity Management in Europe for Life
PET	Privacy-Enhancing Technology
SC	Smart Card
TPM	Trusted Platform Module.
URL	Uniform Resource Locator

7 Bibliography

[Art29WP100] Article 29 Working Party, "Opinion 10/2004 on More Harmonised Information Provisions", 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf.

[ADFS12] J. Abendroth, V. Liagkou, A. Pyrgelis, C. Raptopoulos, A. Sabouri, E. Schlehahn, Y. Stamatiou and H. Zwingelberg, D7.1 Application Description for Students—Version1,2012,https://abc4trust.eu/download/ABC4Trust-D7.1-Application-Description-Students.pdf

[DCDE12] J J. Abendroth, S. Bcheri, N. Götze,V.Liagkou, M. Orski, R. Seidl and F. Veseli, D5.2 Description of the "Common Denominator" Elements, https://abc4trust.eu/download/ABC4Trust-D5.2-Description-of-the-Common-Denominator-Elements.pdf

[EFP14] S. Bcheri, K. L. Damgård, D. Deibler, N. Götze, H. G. Knudsen, M. Moneta, A. Pyrgelis, E. Schlehahn, M. B. Stausholm and H. Zwingelberg, D5.3 Experiences and Feedback of the Pilots—Vesion1, 2014, https://abc4trust.eu/download/

[SDFBP12] S. Bcheri, N. Götze, V. Liagkou, A. Pyrgelis,C. Raptopoulos, Y. Stamatiou, K. Storf, P. Wängmark and H. Zwingelberg, D5.1 Scenario Definition for both Pilots—Version1, 2012, https://abc4trust.eu/download/ABC4Trust-D5.1-Scenario-Definition.pdf

[ESP14] S. Bcheri and M. Moneta, D6.3 Evaluation of the school pilot, 2014, https://abc4trust.eu/download/

[BKR+13] Z. Benenson, I. Krontiris, K. Rannenberg, D. Schröder, A. Schopf, Y. Stamatiou, and V. Liagkou, "Understanding and Using Anonymous Credentials," poster at the 9th Symposium On Usable Privacy and Security (SOUPS 2013), Newcastle, UK, July 2013.

[DAVIS89] F. D. Davis: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, pages 319-340, 1989.

[DINEV05] T. Dinev, M. Bellotto, P. Hart, C. Colautti, V. Russo and I. Serra, "Internet Users' Privacy Concerns and Attitudes Towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences Between Italy and the United States", 18th Bled E-commerce Conference, Bled, Slovenia, Outstanding Paper Award,2005.

[NHSPSPD] K. Damgaard, H. Ghani, N. Goetze, A. Lehmann V. Liagkou, J. Luna, G. Mikkelsen A. Pyrgelis and Y. Stamatiou, D7.2--Necessary hardware and software package for the student pilot deployment, 2012

[KC05] P. Kumaraguru and L. F. Crano, "Privacy indexes: A survey of Westin's studies", Institute for Software Research. Paper 856, 2005.

[TMA32] R. Likert, "A Technique for the Measurement of Attitudes", Science Press, 1932

[MCKNIGHT11] D. H. Mcknight, M. Carter, J. B. Thatcher, and P. F. Clay, " Trust in a specic technology: An investigation of its components and measures", ACM Transactions on Management Information Systems (TMIS), 2(2):12, 2011.

[PAVLOU03] P. 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.

[ROUSSEAU98] D. Rousseau, S. Sitkin, R. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust", Academy of Management Review, 23, 393–404, 1998.

[WAF12] E. Wästlund, J. Angulo, and S. Fischer-Hübner. Evoking comprehensive mental models of anonymous credentials. In Open Problems in Network Security, pages 1-14. Springer, 2012.