D7.1 Application Description for students

Abendroth Joerg, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Ahmad Sabouri, Eva Schlehahn, Yannis Stamatiou, Harald Zwingelberg

Editors:	*Yannis Stamatiou (Computer Technology Institute)*
Reviewers:	*Norbert Götze (Nokia Siemens Networks), Anja Lehmann (IBM)*
Identifier:	*D7.1*
Type:	*Deliverable*
Version:	*1.0*
Date:	*06/03/2012*
Status:	*Final*
Class:	*Public*

Abstract

This deliverable describes the context as well as the details and requirements of the usage scenarios of the ABC4Trust pilot system that will give the opportunity to university students to remotely evaluate courses they have attended in the semester. The student's eligibility will be checked using Privacy-ABCs and smart card technology while their anonymity will be protected throughout as well as after the evaluation period. The pilot's main goal is to provide feedback to Privacy-ABC technology developers as well as to pave the way towards a more general usage of this technology among members of the educational community in Greece.

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 AS	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-Siemens 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)
Executive Summary	Yannis Stamatiou (CTI)
First Chapter	Vasiliki Liagkou (CTI), Christoforos Raptopoulos (CTI)
Second Chapter	Vasiliki Liagkou (CTI), Christoforos Raptopoulos (CTI), Ahmad Sabouri(GUF)
Third Chapter	Abendroth Joerg(NSN), Vasiliki Liagkou (CTI), Christoforos Raptopoulos (CTI)
Fourth Chapter	Vasiliki Liagkou(CTI), Christoforos Raptopoulos (CTI)
Fifth Chapter	Harald Zwingelberg (ULD), Eva Schlehahn (ULD), Vasiliki Liagkou (CTI), Apostolis Pyrgelis (CTI), Christoforos Raptopoulos (CTI), Ahmad Sabouri (GUF)
Sixth Chapter	Vasiliki Liagkou (CTI)
Seventh Chapter	Vasiliki Liagkou (CTI)
Appendix A	Vasiliki Liagkou (CTI), Christoforos Raptopoulos (CTI)
Appendix B	Vasiliki Liagkou (CTI), Christoforos Raptopoulos (CTI)
Appendix C	Vasiliki Liagkou (CTI), Christoforos Raptopoulos (CTI)

Foreword Executive Summary

This deliverable describes one of the two pilots of the ABC4Trust project which will be conducted in the context of WP7: University course evaluations by certified students. The goal of the pilot is to use privacy enhancing Attribute-based Credentials (Privacy-ABCs) that will allow University students to anonymously participate in an online course evaluation at the end of the semester.

The pilot addresses the special challenge that for important and influential results of a poll to be correct and credible, the privacy of the people expressing their opinion must be preserved. ABC technology will guarantee than no information is sent to the system in the first place, which can later be used to identify the student who submits the evaluation. At the same time, the pilot system will guarantee that only eligible students can have access to the evaluation of a course. That is, the system must first verify that a student (i) is enrolled in the university, (ii) has registered to the course and (iii) has attended most of the lectures of that course. To satisfy the above requirements, each student obtains a smart card, which is used to receive Privacy-ABCs, issued by the university. These credentials will be used by students at the end of the semester to prove the desirable properties, e.g. verify their enrolment in the university and the course they have registered for, without revealing their identity. The students utilize the same smart card to anonymously collect evidence for their class attendance throughout the semester by waving the card in front of a contactless smart card reader installed in the lecture room. At the end of semester, they anonymously authenticate from their PCs to the online evaluation page of the corresponding course, by combining the credentials they have collected.

This deliverable gives the details behind the above general pilot context description and provides details on how the pilot requirements given in deliverable D5.1[DSDBP12] will be transformed into a fully operational system that will support the pilot scenarios. More specifically, in this deliverable we provide the details of the university pilot environment, the chosen use cases and the ABC functionalities required for their implementation, the pilot architectural elements, their interactions, and impact of the pilot as well as the relevant legal considerations. Finally, in the appendix, we provide a user manual that will be distributed to the students in order to acquaint them with the pilot and its goals.

Our pilot has as its utmost goal to provide, through the implementation of the course evaluation system end its deployment by the students, feedback to the ABC technology developers on the user acceptance and usability of the technology, from the user's point of view as well as feedback on the ease of development from the developers' point of view. The course evaluation for certified students will provide several additional properties via ABC technologies to students like University registration, revocation authority, storing and backing up their attendance information.

Table of Contents

Index of Figures

Index of Tables

1 Introduction

Over the past 10-15 years, a number of technologies have been developed to build ABC systems in a way that they can be trusted, like normal cryptographic certificates, while at the same time protecting the privacy of their holder (e.g., hiding the real holder's identity). Such Attribute-based credentials (ABCs) are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key. Further details about ABCs technologies can be found in [Kro11]. The ABC4Trust project ([ABC11]) aims to run the first ever pilots of ABC deployments in production environments. Thus this will be the first time real user feedback on ABC systems will be collected. ABC4Trust will gather practical experience with ABC applications in two specific environments. Having these two specific pilots will give the opportunity to test credentials use and performance with two user groups of differing skills and needs. One of the user groups will be students at a Greek university. The University pilot will provide feedback of distinct value to the developers of the reference implementation.

The University pilot will consider remote course evaluation within universities. The students of a Greek university will be issued credentials that certify a number of facts about them (e.g. name, matriculation number, etc.), allowing student with proper credentials to anonymously provide feedback on courses and professors they had during a semester. To be eligible to participate, the students' credentials should prove some facts about them, i.e. whether they have taken the course and they have sufficient number of course attendances.

In the deployment of the University Pilot two essentially different credential technologies (namely the U-Prove of Microsoft and the Identity Mixer of IBM) will be integrated in a single platform. The purpose of the University Pilot is to experiment with all the aspects of these technologies, provide feedback for improvements and offer an overall assessment of their applicability, usability and effectiveness. In the following sections we describe environment and the users of the Pilot.

By taking into account the design / implementation of the necessary infrastructure (Identity Service Provider, infrastructure to issue credentials [e.g. based on smart cards], attribute databases, etc.), the evaluation of these pilots will provide a clear proof of concept of both the unified anonymous credentials idea (harmonization of various ABC protocols) as well as the "Architecture" (WP2) and "Reference Implementation" (WP4), providing at the same time feedback for enhancements. The pilot will especially provide valuable feedback to the ABC system designers towards the second version of the architecture.

1.1 The ABC4Trust Project

The aim of ABC4Trust is to deepen the understanding in a unified approach of ABC technologies (using two distinct ABC engines), enable their efficient/effective deployment in practice, and their federation in different domains. To this end, the project:

1. Produces an unified architectural framework for ABC technologies that allows different realizations of these technologies to coexist, be interchanged, and federated

    a. Identify and describe the different functional components of ABC technologies, e.g. for request and issue of credentials and for claims proof;

    b. Produce a specification of data formats, interfaces, and protocols formats for this framework;

2. Defines criteria to compare the properties of realizations of these components in different technologies; and

3. Provides reference implementation of each of these components.

With a comparative understanding of today's available ABC technologies, it will be easier for different user communities to decide which technology best serves them in which application scenario. It will also be easier to migrate to newer ABC technologies that will undoubtedly appear over time. In addition the same users may want to access applications requiring different ABC technologies, and the same applications may want to cater to user communities preferring different ABC technologies.

Hence, it is also necessary that different ABC technologies be able to coexist or be interchanged across scenarios involving the same users and application platforms. It may also be sometimes desirable to convert ABCs from one technology into another so as to federate them across different domains, as is done today between different authentication domains using standards such as SAML, WS-Trust, Kerberos, OpenID, or OAuth. There are no commonly agreed sets of functions, features, formats, protocols, and metrics to gauge and compare ABC technologies, so it is hard to judge their respective pros and cons. There is also currently no established practice or standard to allow for the interchangeability and federation of ABC technologies.

A number of countries have already introduced or are about to introduce electronic identity cards (eID) and drivers licenses. Electronic ticketing and toll systems are also widely used all over the world. As such electronic devices become widespread for identification, authentication, and payment (which links them to people through credit card systems) in a broad range of scenarios, the users' privacy and traceability will be increasingly threatened in the future internet society. If and when eIDs are rolled out, society and countries are well advised to build privacy protection techniques into them. Privacy-ABCs are a suitable way to mitigate a series of privacy related risks in eID environments and a wide availability of the technology would be beneficial for the privacy and security of citizens [ZwiHan2012].

1.2 Attribute-based Credentials

A *credential* is a certified container of attributes issued by an Issuer to a User (i.e. an entity possibly collecting credentials from various Issuers and controlling which information from which credentials she presents to which verifiers). An attribute is described by the *attribute type*, determining the semantics of the attribute (e.g., first name), and the *attribute value*, determining its contents (e.g., John). By issuing a credential, the Issuer vouches for the correctness of the contained attributes with respect to the User.

The User can then later use her credentials to provide certified information to a Verifier (for authentication or an access decision), by deriving *presentation tokens* that reveal partial information (in fact the minimum required information needed for the transaction) about the encoded attributes. Apart from revealing information about credential attributes, the presentation token can optionally sign an application-specific message and/or a random nonce to guarantee freshness. Moreover, presentation tokens support a number of advanced features such as pseudonyms, device binding, inspection, and revocation.

Presentation tokens based on Privacy-ABCs are in principle cryptographically unlinkable (although naturally, they are only as unlinkable as the information they intentionally reveal) and untraceable, meaning that Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials and that Issuers cannot trace a presentation token back to the issuance of the underlying credentials. However, pseudonyms and inspection can be used to purposely create linkability across presentation tokens (e.g., to maintain state across sessions by the same User) and create traceability of presentation tokens (e.g., for accountability reasons in case of abuse).

There are a handful of proposals of how to realize an ABC system in the literature [Cha85, Bra93, CL01, CL04]. Notable is especially the appearance of two technologies, IBM's Identity Mixer and Microsoft's U-Prove, as well as extended work done in past EU projects. In particular, the EU-funded

projects PRIME and PrimeLife have actually shown that the state-of-the art research prototypes of ABC systems can indeed confront the privacy challenges of identity management systems.

The PRIME project has designed an architecture for privacy-enhancing identity management that combines anonymous credentials with attribute-based access control, and anonymous communication. That project has further demonstrated the practical feasibility with a prototypical implementation of that architecture and demonstrators for application areas such as e-learning and location-based services. PRIME has, however, also uncovered that in order for these concepts to be applicable in practice further research is needed in the areas of user interfaces, policy languages, and infrastructures.

The PrimeLife project has set out in 2008 to take up these challenges and made successful steps towards solutions in these areas. For instance, it has shown that ABC systems can be employed on Smart Cards and thus address the requirements of privacy-protecting eID cards [BCGS09]. Also, in the last decade, a large number of research papers have been published solve probably all roadblocks to employ ABC technologies in practice. This includes means to revoke certificate [Ngu05, BDDD07, CL02, CKS09], protection of credentials from malware [Cam06], protection against credential abuse [CHK+06, CHL06], proving properties about certified attributes [CG08, CCS08], and means to revoke anonymity in case of misuse [CS03].

Despite all of this, the effort of understanding ABC technologies so-far was rather theoretical and limited to individual research prototypes. Indeed, so far, PRIME and PrimeLife only showed that ABC technologies provide privacy-protection in principle.

Furthermore, there are no commonly agreed set of functions, features, formats, protocols, and metrics to gauge and compare these ABC technologies, and it is hard to judge the pros and cons of the different technologies to understand which ones are best suited to which scenarios.

Thus, there is still a gap between the technical cryptography and protocol sides of these technologies and the reality of deploying them in production environments. A related problem with these emerging technologies is the lack of standards to deploy them. As a result the ENISA paper mentioned above observes that ABC "technologies have been available for a long time, but there has not been much adoption in mainstream applications and eID card applications" even though countries such as Austria and Germany have taken some important steps in this sense.

1.3 The University Pilot

Course evaluations have become standard practice in most universities around the world. However they are typically conducted on paper to protect the students' privacy. In cases where they are conducted through computers, the computers are operated by a neutral trusted organization independent from the school doing the evaluation; otherwise the students need to put a lot of trust in the fairness and privacy practices of their university.

The University pilot addresses this special challenge: for important and influential results of electronic course evaluation to be correct and credible, the privacy of the people expressing their opinion must be preserved. Therefore, ABC technology is employed to guarantee that a legible student participates in the course evaluation anonymously without revealing his private and personal information. At the same time, the system must guarantee that only eligible students can have access to the evaluation of a course. That is, the system must first verify that a student (1) is enrolled in the university, (2) has registered to the course and (3) has attended a sufficient number of the lectures of that course.

To satisfy the above requirements, each student obtains a smart card, which is used to receive Privacy-ABCs, issued by the university. These credentials will be used by students at the end of the semester to prove the desirable properties, e.g. verify their enrolment in the university and the course they have registered for, without revealing their identity. The students utilize the same smart card to anonymously collect evidence for their class attendance throughout the semester by waving the card in front of a NFC device installed in the lecture room. At the end of semester, they anonymously

authenticate from their PCs to the online evaluation page of the corresponding course, by combining the credentials they have collected. The technology behind the scene does not allow the card owners to exchange their obtained credentials or submit more than one final evaluation for the same course.

As a result of this technology, universities will be able to run their own online course evaluation systems that increase the trustworthiness between the students and the university. The goal of the pilot is to gather information on the reactions of a typically critical group of users. Most importantly, it will provide concrete feedback on the user acceptance and usability of the technology, something that has not been done for this technology before.

1.3.1 University Pilot Objectives

The objectives for the University Pilot are:

1. Schedule and conduct the Student Evaluation scenario.
2. Define success criteria for the Student Evaluation scenario.
3. Provide feedback to the architecture and reference implementation.
4. Provide evaluation results useful to Users, Identity Service Providers, Relying Parties, and Standardization Bodies.

The ABC4Trust framework will be demonstrated through student evaluations of instructors and courses in higher education institutions. With respect to (1) the evaluations are an important tool for universities and governments for correcting and adjusting the curricula so as to correspond best to students' needs. In the University pilot the ABC4Trust framework will allow evaluations over the Internet which will facilitate greatly the evaluation process.

With respect to (2), the University pilot of the ABC4Trust framework will define the success criteria compared to the classical process based on paper evaluation forms. With respect (3), it is important to get feedback from students and professors for the course evaluation with regard to several usage criteria of the ABCs credentials concept as well as the reference implementation. With respect to (4), the University pilot will gather information on the user acceptance and usability of the technology.

The Student Evaluation scenario of the ABC4Trust framework will a) allow the students to evaluate courses, b) automatically archive the evaluation results in electronic form allowing their further electronic processing, and c) offer the possibility of using strong cryptographic tools to ensure student anonymity and data confidentiality.

However, the major challenge is to ensure that only registered and eligible (e.g. to have attended over 2/3 of the course classes) students participate while not forcing them to provide details which may reveal identifying personal information. This requirement can be satisfied using attribute based credentials over the reference implementation of the project where for each student a set of credentials will be defined in the context of the project that allow proving their eligibility for participating in a specific evaluation (e.g. proof that they are indeed students of the department offering the course, proof that they are registered to the course under evaluation and proof that they have attended sufficient number of classes, without, however, revealing the exact attendance ratio). The student credentials will be stored in smart cards and will be used to certify certain student properties (this scenario requires that the students use a smart card reader at the computer they use to provide their evaluations). The University Pilot will conduct an on-site testing and two rounds of Course Evaluation by certified students

1.3.2 Scope and Goals of the Pilot

University Pilot focuses on the execution of a course evaluation in order to try out, assess and provide feedback on ABC systems. The first goal of the University Pilot is to address the description of the usage criteria for the scenario of course evaluation and the overall description of the application for students.

The University Pilot will be one of the first ever pilots of ABC deployments in production environments. Thus this will be the first time real user feedback on ABC systems will be collected. University Pilot's scope is to gather practical experience with ABC applications in the specific environment of a Greek University. The experience to be gathered by this Pilot (together with the experience to be gathered from the Swedish Pilot) will give the opportunity to test credentials' use and performance with two user groups of differing skills and needs. The user group for the University Pilot will be students at a Greek university. The University Pilot will provide feedback of distinct value to the developers of the reference implementation.

More specifically the University Pilot will consider remote course evaluation within universities. In order to achieve the objectives presented in Section 1.3.1 we have defined the following intermediate goals:

1. Describe the plans for the activities that will be performed in University Pilot, the assessment procedures that will be followed, the meetings that will be arranged involving the pilot's platform as well as the users of the platform.
2. Provide indicative usage scenarios that will be used in the Pilot of the ABC4Trust framework, and present some security critical functionalities of technologies employed in the pilot (namely U-prove and Identity Mixer). These functionalities will later be modelled in order to analyse the security aspects involved.
3. Describe the usage criteria for the evaluation, as applied in the context of the University pilot's application

1.4 Description of the Pilot Environment

The University Pilot will take place in the Computer Engineering and Informatics Department of the University of Patras in Greece. This is one of the most highly esteemed departments related to computer science in Greece. It is located very near to CTI premises. For the purposes of the University Pilot, a group of 25 students will take part in the evaluation of the following two courses:

1. Operating Systems Laboratory: This is a compulsory course that takes place at the 6th semester and the number of students that attend it is approximately 200.
2. Distributed Systems I: This is a non-compulsory course that takes place at the 7th semester and the number of students that attend it is approximately 60.

Course evaluations are a standard practice in Greek universities and are supported by the Hellenic Quality Assurance Agency for Higher Education (HQAA). The purpose of HQAA is to ensure the transparency of the evaluation procedure and also to guarantee that these procedures will be used in enhancing the quality of higher education.

However, up to date course evaluations in Greece are conducted on paper and they are done after class inside the lecture room. This unfortunately hinders the whole procedure, since the students need to put a lot of trust in the fairness and privacy practices of their university.

The University pilot realizes an electronic course evaluation in a way that ensures the credibility of results and preserves the privacy of the students expressing their opinion. More specifically, the system scope will be the realization of a course evaluation where university students can anonymously rate courses they took while ensuring that: 1) participants are valid University of Patras students 2) participants are students that have indeed registered to the course and have had sufficient attendance and 3) participants can only rate the course once, without keeping list of students who have already rated the courses, so as to protect student anonymity.

1.4.1 User Community Description

In University Pilot the course professors will upload the questionnaires regarding their course and determine the threshold number of attended lectures required for participating in the evaluation. This activity does not require ABC technology. Students will be able to evaluate courses that they have registered to and attended. When the evaluation procedure is completed, CTI members will collect and process the evaluation results in order to provide accumulated course evaluation results to HQAA. This off-line activity does not require ABC technology. Table 1 presents several properties for each User group present in the University Pilot.

User Group	Description / Expected Use of System	Geographic Location	Network Profile (LAN, WAN, External)	Total Users	Concurrent Users
Students	Certified Course Evaluation	University/ Home	LAN, WAN	25	25
Professor	Upload Evaluation Questionnaire	University/ Home	LAN, WAN	2	1
CTI	Collect and Process Evaluation Results	CTI	LAN, WAN	2	1
HQAA	Access Accumulated Evaluation Results	University	LAN, WAN	1	1
Department Registration Employee	Import Students Data	University	LAN	1	1
Administrator	System Administration	CTI/NSN	LAN, WAN	3	1
Phd Students	NFC setup	CTI		2	2

Table 1: Physical/Legal Roles

1.4.2 Short Description of CTI Network Infrastructure

CTI has a modern corporate network located in three different sites: The main site is the building "D. Maritsa" Campus of the University of Patras and the other two smaller ones are at Patras University (Building B) and at the Athens CTI premises. The connection between the sites is realized by optical fiber between the building "D. Maritsa" and Patras University and by virtual private networking (vpn) with capacity 15Mbps between building "D. Maritsa" and Athens CTI premises.

CTI is connected to the Internet through GRNET using a 1 Gbps speed connection by optical fibers in the building "D. Maritsa". CTI has its own public address space with 32766 available IP addresses and BGP autonomous system. The network security is ensured by the existence of a pair of firewalls (cisco pix-535) which are connected to high availability configuration (active-standby). The firewalls are connected between the CTI border router and the CTI internal network, and check incoming and outgoing traffic, ensuring network security and protection against malicious attacks.

CTI's internal network uses structured cabling and Ethernet UTP cat6 is fully gigabit switched. To improve performance and security the network is divided into virtual LANs (vlans) in which there are connected network devices, servers and workstations. In the building "D. Maritsa" there are 2 routers which take over routing in the vlans inside the organization, 1 hub for central computer systems and 4 hubs for the connection of users. The active network ports in the building "D.Maritsa" are around 600. For the Patras University and Athens CTI premises sites the active ports are 50 and 170 respectively.

1.5 Structure of the Document

The purpose of this document is to give a general preview of the planned deployment and operation of the University Pilot. It provides the details of the university pilot components and environment, the chosen use cases and the ABC functionalities required for their implementation, the pilot architectural elements, their interactions, and impact of the pilot as well as the relevant legal considerations. Finally, this document includes a proposed user manual suitable for students in order to familiarize them with the pilot and its goals.

In this chapter we introduced the ABC4Trust Project and the University Pilot. Moreover we gave an overview of the University Pilot, a general description of the Pilot environment and CTI's network and a presentation of the basic actors involved.

The rest of this document is organized as follows:

Chapter 2 presents the use case scenarios needed for describing the general Pilot's functionality from the users' perspective.

Chapter 3 provides a high level description of the architecture of the University Pilot System, as well as detailed description of its components.

Chapter 4 presents the timeline related to the deployment and realization of the Pilot.

Chapter 5 gives a detailed description of various requirements. Moreover it gives a description of required attributes in the Credentials. Finally, we present all the useful information from related parts of the D5.1 document [DSDBP12], in order to clarify all the operations that take place in the Pilot.

Chapter 6 focuses on the impact of the evaluation process will have in Greek community and in University Department. Moreover the first feedback from students and professors opinion about University pilot and ABC technologies is presented.

2 Use cases

In this chapter we describe the University pilot's usage scenarios that describe the general functionality of the system from the users' perspectives. We use the following basic scenarios that provide step-by-step descriptions of how the proposed system should operate and interact with its users under a given set of circumstances.

- The first scenario includes the set-up phase, after which all the systems are initiated and also the students of Computer Engineering and Informatics Department have in their possession a smart card with a user secret.
- The second scenario describes the procedures required so that the students can obtain credentials that certify a number of facts about them.
- The third use scenario collects the attendance information of students.
- In order to handle loss of smart card and retrieve the attendance data stored in students' smart cards, we define the next use case scenario that backups and restores students' attendance information.
- The last and basic use case scenario considers the course evaluation within the University of Patras.

2.1 Description of the Use Cases

In the following sections we provide a high level description for the various use case scenarios pertaining to the University Pilot. We begin by describing the ABC System Setup and then we present the scenarios for obtaining credentials for the University/Course Registration and Class attendance data. We also describe the scenario for backing up and restoring Class attendance data, as well as revoking a student's Privacy-ABCs. Finally, we describe the course evaluation scenario.

2.1.1 Preparation of Students SC and System Components

This section describes the preparation of students' smart cards and system components. It provides a high level description of the procedure through which the user secrets of all the participated students, as well as the keys and the parameters of all the system components are generated.

This scenario can be triggered by two main events described below:

The student obtains her smart card and her smart card reader. In particular, the University Registration office distributes a sealed envelope, a smart card and a slip of paper containing a password to each student that participates to the University pilot. The sealed envelope is marked with the smart card ID and contains a PIN and a PUK. The slip of paper associates the envelope's identification number i.e. the smart card ID (provided to student) and the password. The smart card does not contain any personal information at that point. The University Registration office maintains a list of the correspondence between student names, envelope identification numbers with corresponding passwords. The preparation of smart cards is shown in Figure 1.

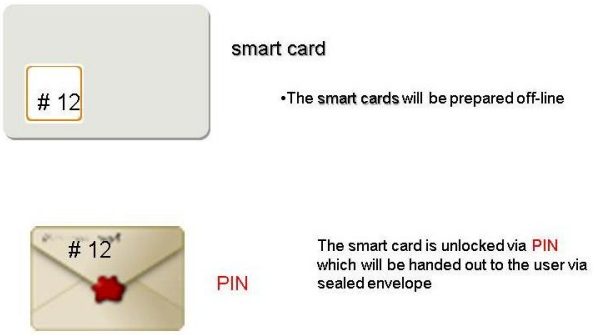

Figure 1: Preparation of Smart Cards

The administrators of the Course Evaluation System, the University Registration System and the Class Attendance System initiate the operation of the corresponding systems for the first time. In particular, CTI with the collaboration of the University Registration office, feeds the IdM database with the students' names and their corresponding envelope identification numbers (distributed to each student) and with the following certified attributes collected from the volunteering students that participate to the University pilot: (a) first name and last name, (b) University Name, (c) Department Name, (d) Matriculation Number. The preparation of IdM database is shown in Figure 2.

At this point, each system administrator does the following:

- He generates the issuer parameters and the issuance keys for the issuers she is responsible for. In particular, this is done for the University Registration System and Class Attendance System.
- The issuer parameters of the University Registration System are stored on the IdM public Directory and can be accessed by the ABC systems.

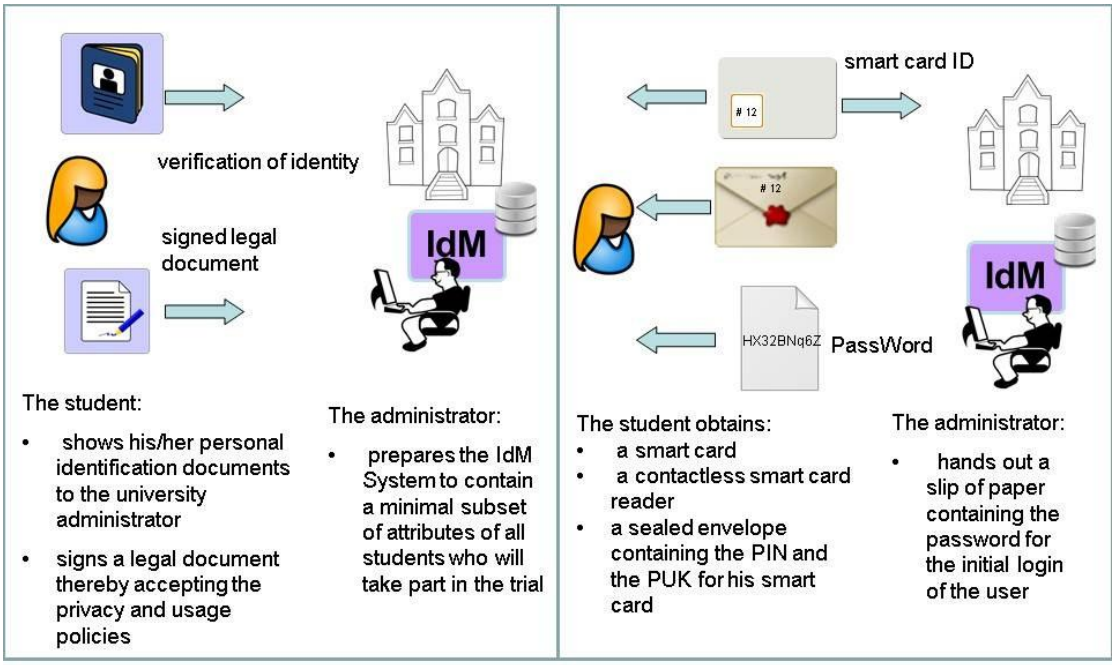

Figure 2: The Two Phases of IdM Preparation

At some point after the parameters and the issuance keys are generated, each student participating in the University pilot can do the following (assuming the appropriate ABC software is installed on student's PC): She puts her smart card on the contactless card reader and starts the initialization of the smart card, which requests her smart card PIN. In particular, the user secret will be generated and will be locked into the smart card. Figure 3 describes ABC system set up.

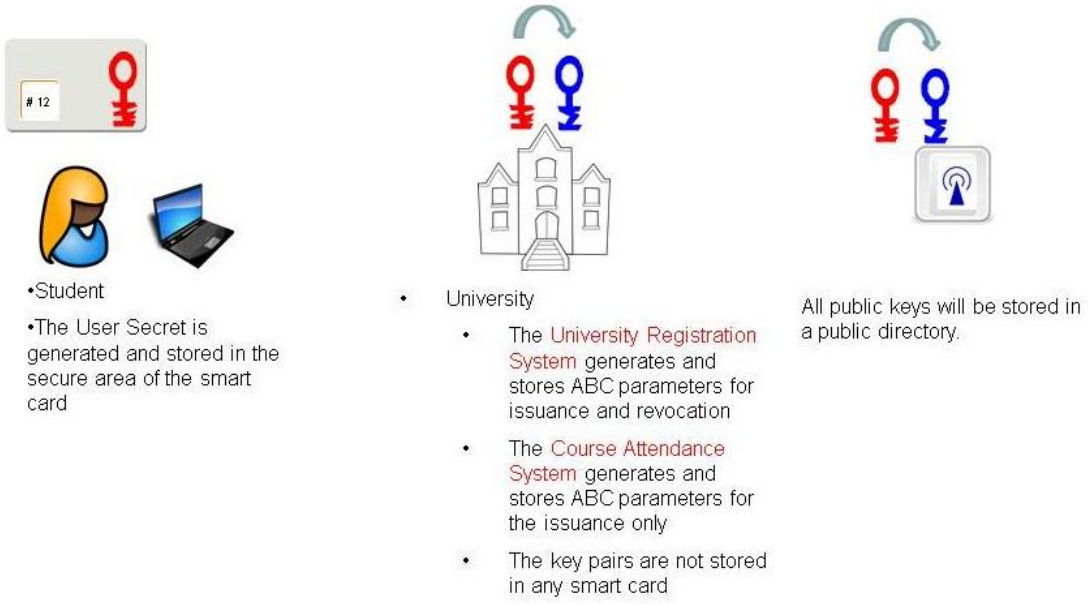

Figure 3: ABC System Setup

2.1.2 Obtaining the University/Course Registration Credential

This scenario describes the steps that a student has to follow in order to be registered at University or enrol in a course. When a student wants to register at the University and obtain a valid student credential, she navigates to the Patras portal and follows the provided instructions. University Registration system authenticates the student and stores a valid student ABC credential on her smart card (see Figure 4). The student credential contains attributes related with personal student information (e.g. first name, last name, matriculation number, see Section 5.8).

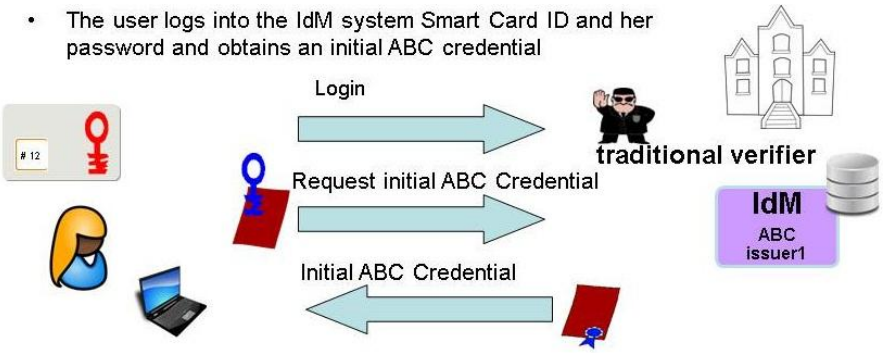

Figure 4: Obtaining the University Credential

As shown in Figure 5, for a student to book a course and obtain a valid course credential, she has to browse the Patras portal and follow the given instructions for booking the course. Student will get a valid course credential in her smart card by logging in the University Registration system via ABC technology. The course credential stored in her smartcard contains attributes related with course information (e.g. course identifier).

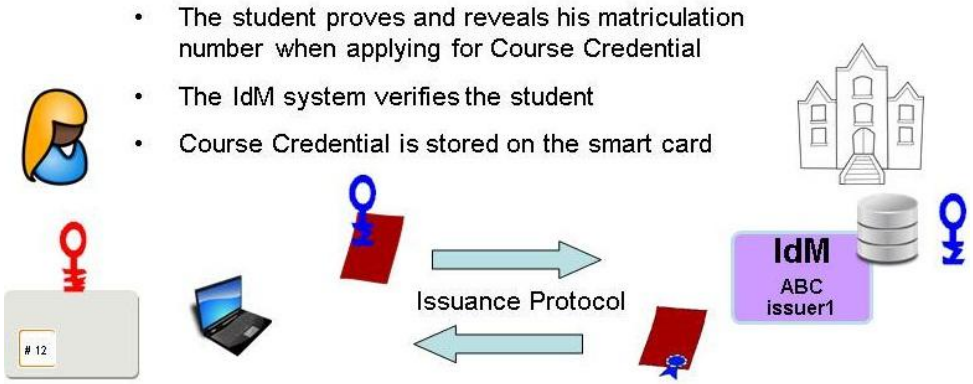

Figure 5: Obtaining Course Credential

2.1.3 Obtaining Class Attendance Data

This scenario uses the Class Attendance system presented in pilot's architecture in order to collect students' attendance information. Since Setup phase has finished all the students who will participate in the evaluation of the two courses, have been issued Privacy-ABCs that certify students' information (first name, last name, etc.) and information related with the course. Students can log in to the IdM portal and can view and administrate some of their data using the acquired credentials (see Figure 6).

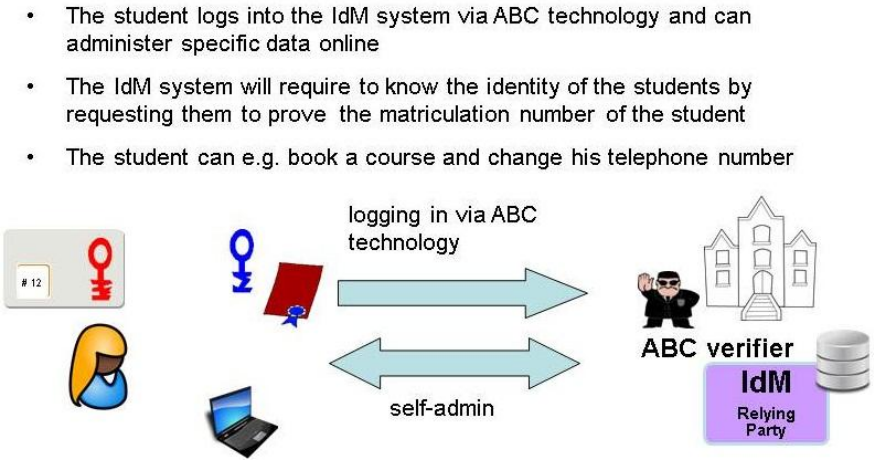

Figure 6: Self Administration of Students Data

Class Attendance System will be placed in the lecture room 15 minutes before the lecture starts and will be available for 30 minutes starting from 15 minutes before the end of the lecture. The Professor is responsible for fixing the exact time when each lecture takes place (location, date, start and finish time). CTI in cooperation with PhD students will be responsible for the Class Attendance System's operation and physical security. Each student has to wave her smart card in front of a contactless NFC

reader when leaving the lecture hall, in order to collect her attendance information. Information in the student's smart-card gets updated every time she attends a class (see Figure 7). It is important that attendance data should not be copied and transferred to absent smart cards.

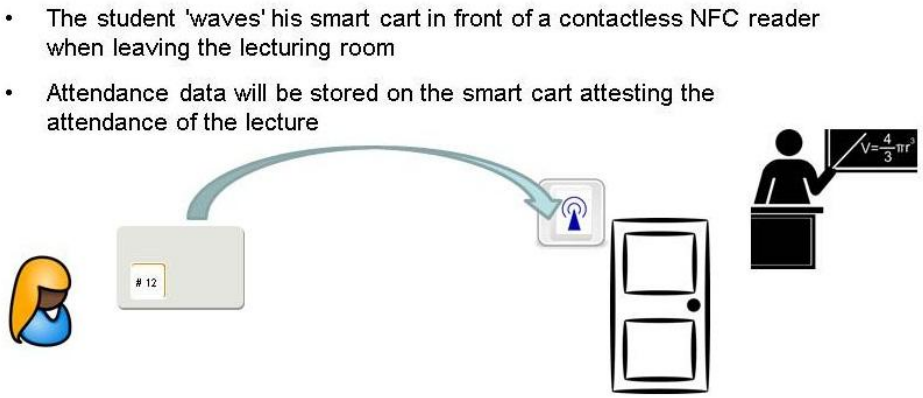

Figure 7: Obtaining Class Attendance Data

2.1.4 Backup of Smart Card Content

This scenario is used in order to handle the loss of a smart card containing student's attendance information. This scenario allows a student to back up her smart card content.

We assume that the student has attended some course lectures (see obtaining class attendance scenario) and has some attendance information stored on her smartcard. Student could run an application locally on her PC in order to browse the Privacy-ABCs stored on her smart card and backup the smart card content on her PC. Figure 8 describes the backup procedure.

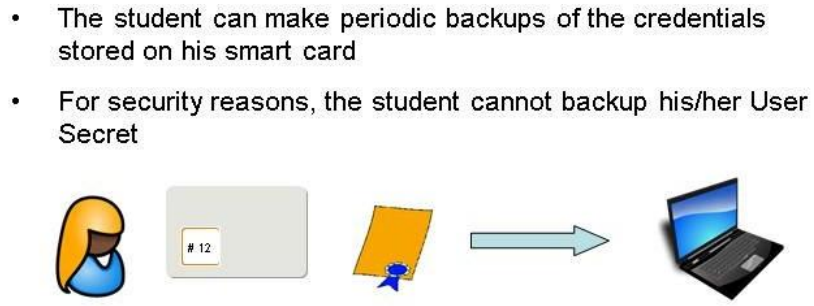

Figure 8: Backup SC Data

2.1.5 Restore of Class Attendance Data

This scenario allows a student to restore backed up data on her (new) smartcard. If a student loses her smartcard then she can declare it lost, and can get a new envelope and smart card from the University Registration Office. If a student has a backup of the old smart card content on her PC, she will be able to restore them into her (new) SC using the User Agent application (see Figure 9). Student should connect her smart card reader to her PC before starting restore procedure. Note that the backup information is stored in encoding format by SC software.

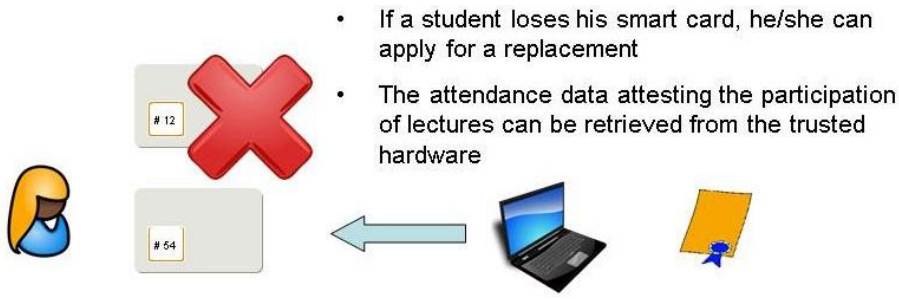

Figure 9: Restore Attendance Data

2.1.6 Revoking a Student's Privacy-ABCs

In some cases the University registration office has to be able to revoke a student's credential. As a first example, when a student has lost her smart card, she must declare her smart card lost to the University Registration Office where she can get a new envelope (containing PIN, PUK) and a smart card. The University Registration System Administrator revokes the student University credential and deletes her private information from the ABC system. Then the student has to obtain a valid student and course credential and she will be able to use the backup data from her PC.

As a second example, when a student graduates and she is no longer enrolled as student, the University registration office has to be able to revoke student's credential. The University Registration System Administrator revokes the student University credential and deletes the related information from the ABC system.

2.1.7 Course Evaluation

Tow group of students will take part in the evaluation of two courses they have attended at a University Department. We assume that the set up phase has been finished and all the students that will participate in the evaluation have at their possession a valid student credential and one or more course credentials. Then only students who can prove sufficient attendance of a specific course may participate in the evaluation process of this course. Thus the students should have stored sufficiently many attendance credentials in their SC.

Before the end of semester the HQAA will cooperate with the Department in order to distribute a general template of course evaluation questionnaire to the professors. Each professor has to customize the course evaluation questionnaire to suit the course's needs. After this, the professor submits the course questionnaire using the course evaluation application. After the final exam has taken place, the students will be able to evaluate the course at any time from their home. Each student should have an ABC4Trust SC reader and have installed the ABC user agent on her computer in order to start the course evaluation procedure. Students are able to participate anonymously in a course evaluation by logging in to the Course Evaluation System via ABC technology. Whenever a student wants to evaluate a course she can access the Patras portal though her computer and the smart card reader. Then the Patras Portal will redirect her to the course evaluation system where only users satisfying certain policies will be able to access. If the Course Evaluation System is not online or if the Course Evaluation System is not yet enabled, the student will receive the proper notification. As shown in Figure 10, the student will be able to fill in the uploaded questionnaire if she satisfies the following policies:

- The student is a Patras University student
- The student has indeed booked the course
- The student has collected sufficient attendance credits during the semester

When a student satisfies these policies the Course Evaluation System prompts the student to fill in the evaluation form and stores the result of the last submitted course evaluation. If the student does not satisfy all the above three policies, she will receive a notification and the evaluation process will be terminated.

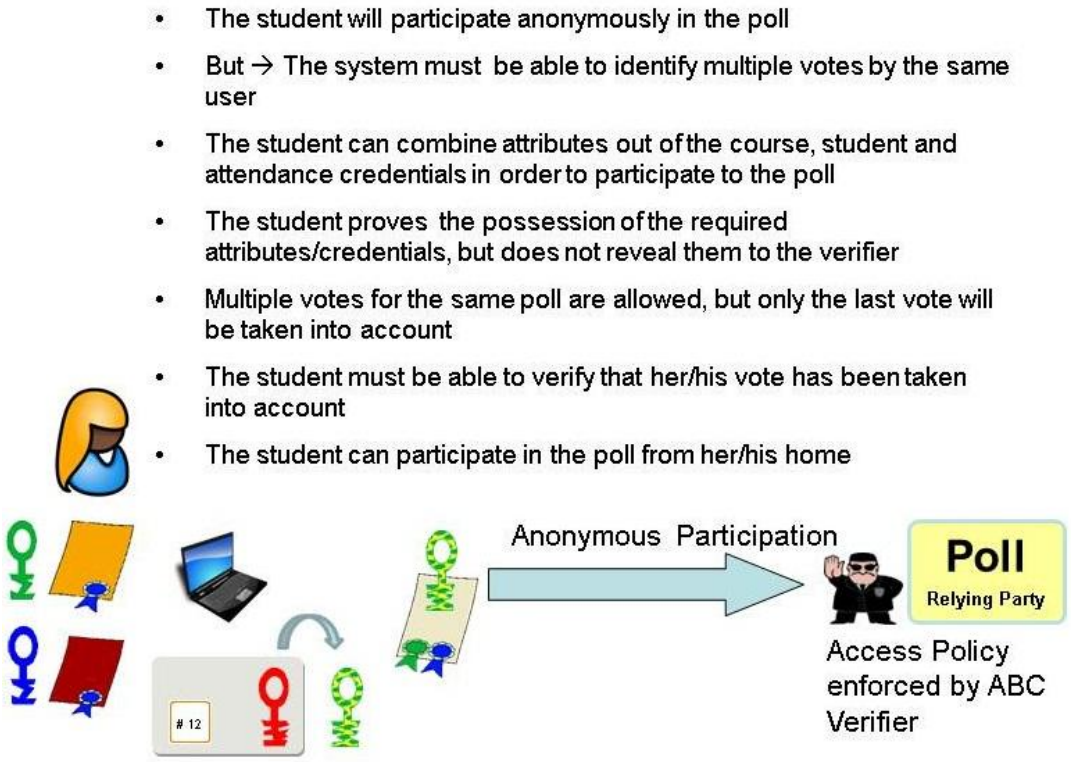

Figure 10: Course Evaluation

Each student is allowed to evaluate multiple times but only the last evaluation is taken into account (to ensure that the student's evaluation was not a result of coercion). The Course Evaluation Application will consist of a database for storing policies and evaluation data. If the policies that specify the eligibility of students to answer a question lead to a small and possibly identifiable subset of students, then the system should prevent the students from answering the question. The HQAA will be invited to cooperate with the Department for the dissemination of the evaluation results.

2.2 Use Cases Detailed Description

In this section, we give a detailed description of the functionalities for the use case applications that were described in Section 2.1. In Section 2.2.1 we give a graphical representation of all use cases, then in Section 2.2.2 we give some useful notations for use case description and finally we give a detailed representation of each use case application.

2.2.1 Use Case Overview

Figure 11 gives a graphical representation of the flaw and the interconnections between all the presented use cases.

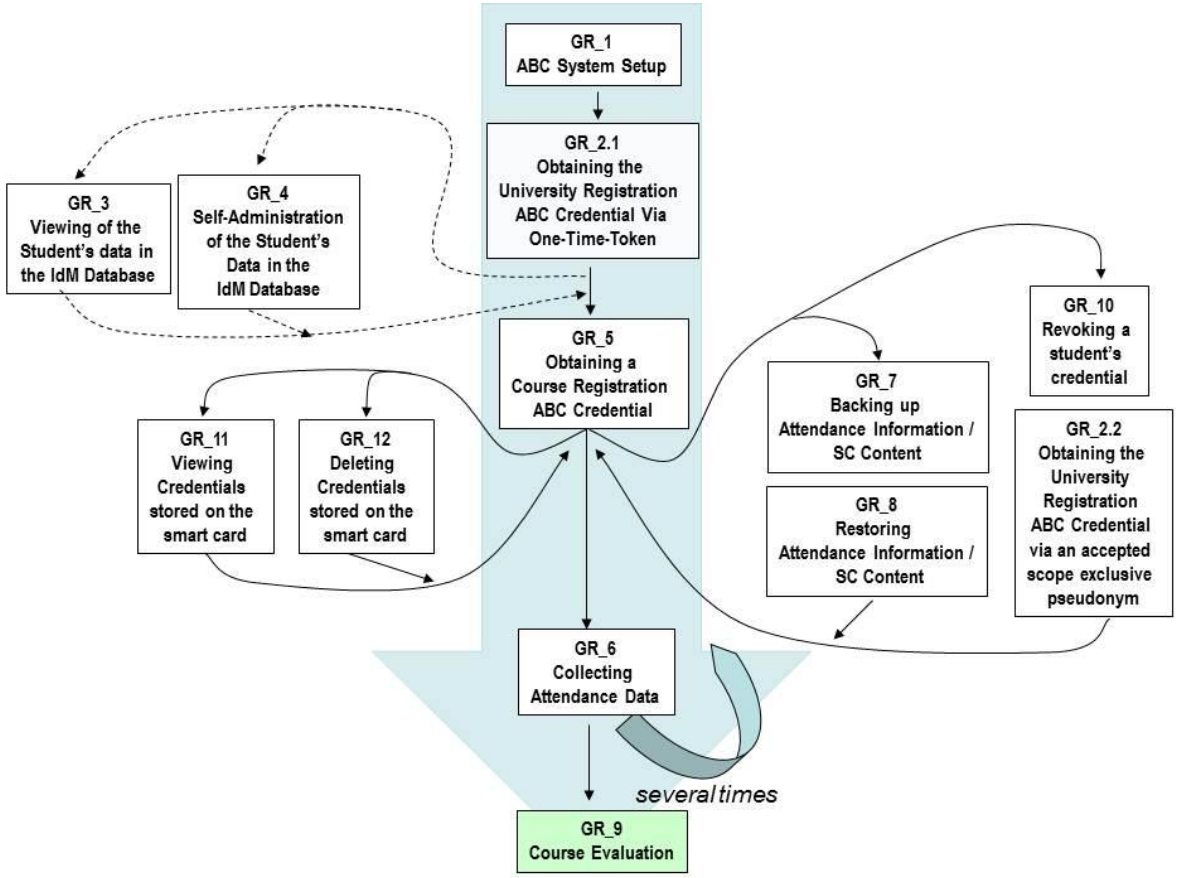

Figure 11: Use Cases Flow

2.2.2 Use Case Identification

In this subsection we present some useful notations and definitions for the following use case description.

2.2.2.1 Use Case ID

We give each use case a unique integer sequence number identifier. We use an incremental form: GR_#.

2.2.2.2 Use Case Name

We state a concise, results-oriented name for the use case. These reflect the tasks the user needs to be able to accomplish using the system. Include an action verb and a noun. Example: System Set up

2.2.2.3 Use Case Definition

- Actors: An actor is a person or other entity external to the software system being specified who interacts with the system and performs use cases to accomplish tasks. Different actors often correspond to different user classes, or roles, identified from the customer community that will use the product. Name the actor that will be initiating this use case and any other actors who will participate in completing the use case.
- Trigger: We identify the event that initiates the use case. This could be an external event or system event that causes the use case to begin, or it could be the first step in the normal flow.

2.2.2.4 Description

We provide a brief description of the reason for and outcome of this use case, or a high level description of the sequence of actions and the outcome of executing the use case.

2.2.2.5 Preconditions

We list any activities that must take place, or any conditions that must be true, before the use case can be started. We number each precondition. Examples:

- The student has installed the ABC software on her PC.
- The student has received a SC.

2.2.2.6 Postconditions

We describe the state of the system at the conclusion of the use case execution. We number each postcondition. Examples:

- The student will have a valid Credential in her SC which indicates that she is a registered student.

2.2.2.7 Normal Flow

We provide a detailed description of the user actions and system responses that will take place during execution of the use case under normal, expected conditions. This dialog sequence will ultimately lead to accomplishing the goal stated in the use case name and description. This description may be written as an answer to the hypothetical question, "How do I <accomplish the task stated in the use case name>?" This is best done as a numbered list of actions performed by the actor, alternating with responses provided by the system. The normal flow is numbered "X.0", where "X" is the Use Case ID.

2.2.3 ABC System Setup

Use Case ID:	GR_1
Use Case Name:	**System Setup**
Actors:	Users: System Administrators (A CTI employee or a member of the university) Students
Description:	All the parties of the system first need to go through an initialization phase in order to become functional.
Trigger:	The student has obtained a new smart card. The administrators of the Course Evaluation System, the University Registration System and the Class Attendance System are powering up the servers for the first time.
Preconditions:	• The student has installed the 'User Agent App' on her PC. • The student has received a SC. • The student has received a sealed envelope containing the credentials to access the SC.
Postconditions:	For Students: • All the cryptographic parameters, system parameters, secret keys and etc. are configured on the smart card and it is ready to operate in the system.

	For System Administrators: • The following Subsystems have their cryptographic parameters, system parameters, secret keys and etc. properly configured and they are ready to provide the corresponding services: ▪ University Registration System ▪ Class Attendance System ▪ Revocation Authority • All parameters, public keys and certificates will be stored in the IdM Public Directory.
Normal Flow:	GR_1.0: System Administrator : 1. In order to ease the administrative tasks, there will be a specific setup script for the each of the following subsystems: • University Registration System • Class Attendance System • Revocation Authority 2. The system administrator just needs to run the proper script on the corresponding machines to make the subsystem ready and functional. Student: 1. User places her card on her smart card reader. 2. The user starts the 'User Agent App' 3. The user selects 'Initialize SC' 4. The user is requested to authenticate to the SC. 5. The 'User Agent App' performs the initialization. 6. The SC will generate a User Secret which will be locked into the SC 7. The SC will store the certificates of all trusted communication partners in a tamper-proof area. 8. The SC will store the all the necessary cryptographic parameters required for communicating with the existing parties in a tamper-proof area.

Table 2: ABC System Setup

2.2.4 Obtaining the University/Course Registration Credential

Use Case ID:	GR_2_1
Use Case Name:	**Obtaining the University Registration Credential**
Actors:	Students
Description:	This use case describes the steps needed for a student to get the certificate for registration at the University.
Trigger:	• The student has received a new smart card • Some of the student's attributes that appear in the university registration

	certificate have changed in the system.
Preconditions:	• The student has obtained her smart card, her ID with her private information and her contactless smart card reader. • The student has initialized her SC (see GR_1). • The student knows the credentials to access the SC content (e.g. PIN). • The student owns a PC with the 'User Agent App' installed on it. • University Registration System is available and student has still her smart card and her contactless smart card reader. • NSN's IdM can be reached by the student from her home. • The IdM database contains a minimal subset of certified attributes of the students and uses the ID as handle.
Postconditions:	• The student will have a valid Credential in her SC which indicates that she is a registered student. Check this credential for minimal subset of certified attributes (see Section 5.8)
Normal Flow:	GR_2_1.0: 1. The user places her card on her contactless smart card reader. 2. The user browses to the ABC Patras Portal. 3. The User selects the menu 'Get University ABC Credential'. 4. The user logs in via ID and her password. 5. The 'User Agent App' pops up 6. The 'User Agent App' requests the user to authenticate to the SC. 7. The System invalidates the ID and binds the student profile to the SC (to the secret key stored in the SC) so that the user can login with her SC afterwards. 8. The 'User Agent App' and the University Registration System will run a protocol to produce the credential according to the profile of the user in the IdM and store it on the SC. 9. Finally, this credential is stored on the SC

Table 3: Obtaining University Credential

	GR_5		
Use Case Name:	**Obtaining a Course Credential**		
Created By:	Stamatiou/Goetze	Last Updated By:	
Date Created:	21.07.11	Date Last Updated:	
Actors:	Students		
Description:	This use case describes the steps needed after a student has booked the courses. Following this use case, the student will receive a certificate showing her enrolment in the course.		
Trigger:	The student books a course by connecting the University Registration System.		
Preconditions:	• The student gone through GR_2_1 and she is able to authenticate to the		

	System using her SC. • The student knows the credentials to access the SC content (e.g. PIN). • The student owns a PC with the 'User Agent App' installed on it. • At least one course is booked in the IdM database. • The deadline for dropping the courses is over.
Postconditions:	• The student receives a certificate (Credential) showing that she is enrolled in the course.
Normal Flow:	GR_5.0: 1. The user browses to the ABC Patras Portal 2. The user selects the University Registration System 3. User selects the menu 'Obtain Course Credential' 4. The 'User Agent App' pops up. 5. The SC asks the user for authentication. 6. The 'User Agent App' and the University Registration System run a protocol to authenticate the user. 7. The University Registration System looks up the user's profile in the IdM. 8. The 'User Agent App' and the University Registration System run a protocol to issue the credential of course enrolment and store it on the SC.

Table 4: Obtaining Course Credential

2.2.5 Obtaining Class Attendance Data

Use Case ID:	GR_6
Use Case Name:	**Collecting Attendance Data**
Actors:	Students
Description:	This use case describes the steps needed for a student to collect attested attendance data of a lecture of a specific course.
Trigger:	The student 'waves' her smart card in front of a contactless NFC reader when leaving the lecturing room.
Preconditions:	• The student has her smart card with him. • The smart card has been initialized before. • The student leaves the lecturing room max 15mins before and 15mins after the lecture. • Attendance System must be up and running.
Postconditions:	• Attendance data is stored on the student's smart card attesting the attendance of each course lecture.
Normal Flow:	GR_6.0: 1. The student waves the smart card in front of the Smart Card Reader 2. The card authenticates the NFC reader 3. The smart card anonymously receives non-transferable information

	that can be used later to prove the student's attendance in this lecture 4. This information is stored in the smart card 5. If the protocol completes successfully, the smart card reader makes a "beep-1" sound

Table 5: Obtaining Class Attendance

2.2.6 Backup Smart Card Content

Use Case ID:	GR_7
Use Case Name:	**Backing up SC content**
Actors:	Students
Description:	This use case describes the steps needed for a student to back up her periodic SC content.
Trigger:	The user wishes to backup her attendance data in case the SC gets lost or corrupted
Preconditions:	• The user has some attendance data stored on her SC. • The student owns a PC with the 'User Agent App' installed on it.
Postconditions:	• The attendance data are stored on the student's PC or any other external storage.
Normal Flow:	GR_7.0: At home: 1. User places her card on her smart card reader. 2. The user starts the "User Agent App" 3. The user selects Backup procedure 4. The SC asks the user for authentication. 5. The user is requested to choose a password for storing the data on her PC 6. The "User Agent App" performs the backup.

Table 6: Backup Smart Card Content

2.2.7 Restore of Class Attendance Data

Use Case ID:	GR_8
Use Case Name:	**Restoring Attendance Credentials / SC content**
Actors:	Students
Description:	This use case describes the steps needed for a student to restore backed up attendance data on her (new) SC. Old attendance data certifying that a student visited specific lectures can be restored on a new smart card.
Trigger:	The student lost her smart card and obtained a new one.
Preconditions:	• There is backup information previously stored on the student's PC • The student owns a PC with the 'User Agent App' installed on it.

Postconditions:	• The backed up attendance data are transferred from the PC to the SC
Normal Flow:	GR_8.0: At home: 1. User places her card on her smart card reader. 2. The user starts the "User Agent App" 3. The user selects 'Restore of Attendance Credentials 4. The user is requested to enter her password (which she chose for backing up the data on her PC) 5. The SC asks the user for authentication. 6. The 'User Agent App' transfers the backup data to the card. 7. The SC checks if the backup data is authentic and it belongs to the owner of the card. 8. If it passes the check, the smart card commits the changes.

Table 7: Restore of Class Attendance Data

2.2.8 Revoking a Student's Privacy-ABCs

Use Case ID:	GR_10
Use Case Name:	**Revoking a Student's Credential**
Actors:	System Administrator
Description:	The Student's Credential becomes invalid.
Trigger:	A student leaves the university (e.g. not turning up). A student leaves the pilot. A student loses her SC or if the SC has been stolen.
Preconditions:	
Postconditions:	The smart card cannot be used anymore to access the system or participate in the course evaluation.
Normal Flow:	GR_10.0: 1. The University Registration system will be informed about the revocation request (e.g. the student shows up in the office and reports the lost card). 2. The University Registration system sends the revocation information to the revocation authority.

Table 8: Revoking a Student's Privacy-ABCs

2.2.9 Course Evaluation

Use Case ID:	GR_9
Use Case Name:	**Course Evaluation**

Actors:	Students Course Evaluation System
Description:	This use case describes the steps needed for a student to be able to evaluate anonymously for a course.
Trigger:	A course related evaluation is initiated by the university personnel. The university requests the students to participate in the evaluation.
Preconditions:	• There is a Course Evaluation System (Student Evaluation System) with which the student can interact from her home. • The deadline for evaluation is not over yet. • The student has in her possession a valid student credential and qualifying number of attendance recorded on her card.. • The student has a SC reader at home • The student owns a PC with the 'User Agent App' installed on it. • The student possesses the following data: ▪ Student credential ▪ Course credential ▪ Sufficient attendance data
Postconditions:	The students' evaluations of a specific course have been collected.
Normal Flow:	GR_9.0: At home: 1. User places her SC on her smart card reader. 2. User browses to the ABC Patras Portal and selects the menu item 'take part in the course evaluation'. 3. The 'User Agent App' pops up. 4. The SC asks the user for authentication. 5. The 'User Agent App' and the Course Evaluation System run a protocol to prove that the student a. is registered with the university b. is enrolled in the course c. has attended a sufficient number of lectures (can even only be 1 or 2 times) 6. If the proof completes successfully the user gets access to the evaluation form. 7. The user fills the form. If she has done it before, she sees the previously entered values and she can modify them. 8. The Course Evaluation System stores the result of the last submitted course evaluation.

Table 9: Course Evaluation

3 Architecture Building Blocks of the University Pilot

The general architecture of the ABC4Trust pilot as it will be deployed in Patras is depicted in Figure 12 below and further described within this section.

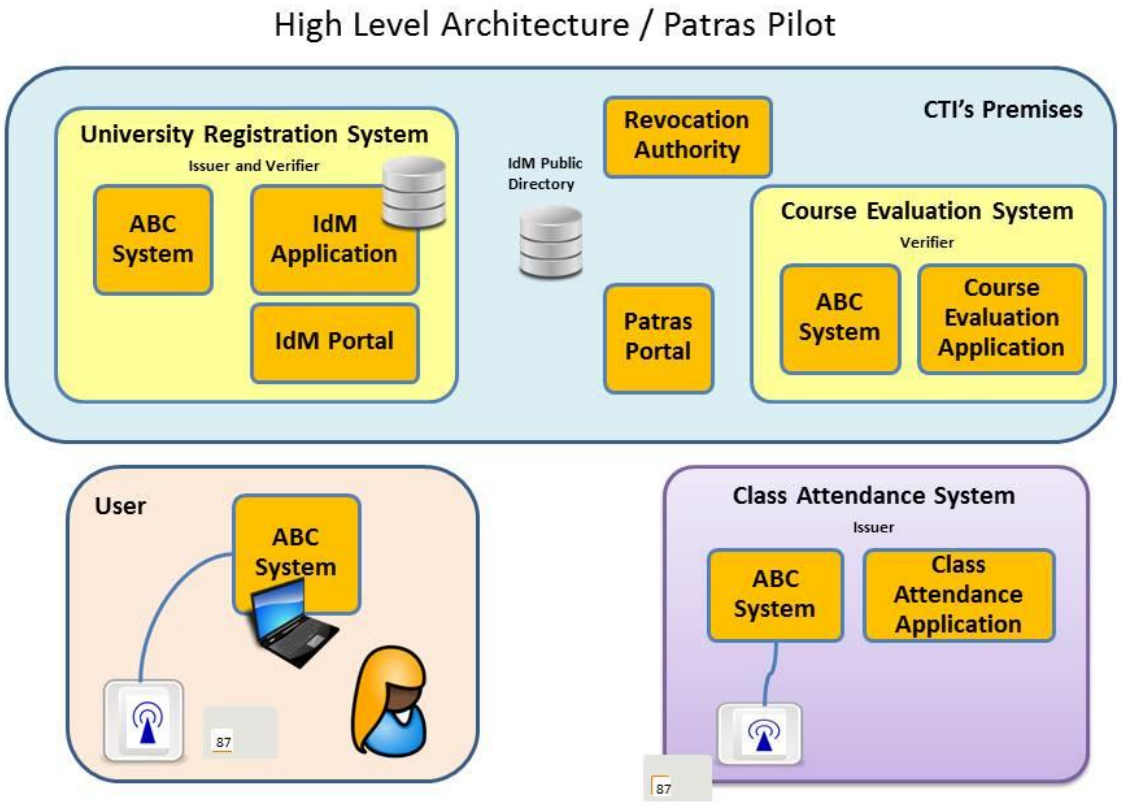

Figure 12: High Level Architecture of the Patras Pilot

3.1 Components Description

As can be seen from Figure 12, the architecture of the Patras pilot is based on various components. These components have different functionalities and roles based on the scenario and use case definition of this pilot. Next, we describe the functionality and the characteristics of each high level component that is presented on the architecture figure. Note that the user interactions with the Patras Portal, University Registration System and Course Evaluation System are online whereas her interactions with the Class Attendance System are offline. The Informational Model of University Pilot is presented in Appendix B. All the components presented in architecture Figure 12 are described in details in this section.

3.1.1 University Registration System

This component is mainly used for issuing Privacy-ABCs to the users of the system. Its sub-components are an ABC System, an IdM Application and the IdM portal. The IdM application is a web application whose potential users are students and university registration office employees. In particular:

- CTI with collaboration of a university registration office employee has the possibility to insert to the database of the University Registration System the personal information of the student-volunteers that will participate in the pilot. This activity does not require ABC technology.
- A university registration office employee can 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).
- Students can collect credentials that certify that they are valid students of the University of Patras
- Students are able to browse their personal data that is stored in the IdM database
- Students are able to administrate some of their personal data (e.g. course)
- Students can collect credentials that certify that they have registered to a course

When the IdM application is required to issue Privacy-ABCs to users (e.g. university credentials, course credentials) it invokes the ABC System which is responsible for performing the issuing protocols. When a user wants to browse her personal information, the IdM portal can be accessed via the IdM application that supports this functionality.

As the University Registration System is the main issuer of the Patras pilot, its parameters (system parameters, revocation information) should be stored in a public repository, so that all system components can access them. This repository is the IdM Public Directory that can be seen on the "High Level Architecture of the Patras pilot" figure.

University Registration System includes the University Registration ABC System, IdM Portal and IdM Application, that are described below:

1. **The University Registration ABC System** is a component of the University Registration System that is responsible for issuing students' credentials. In particular, students can collect their university registration credentials as well as course registration credentials. This application interfaces with the IdM application. More specifically, when a student wishes to get issued a University or a Course credential this application forwards to the IdM application an issuance policy and containing a credential template. This information is forwarded to the user in order for an interactive issuance protocol to take place. The IDM application is responsible to provide to the University Registration ABC System the student attributes that will be part of the credentials.
2. **The IDM Portal** is the frontend the user-facing part of the university registration system. During the early phase of the trial it supports bootstrapping the ABC4Trust system, including selection of courses the students will attend. The IDM portal provides the administration interface to the users, to change their persistent-non-anonymous data. The IdM Portal includes the ABC functionality of an issuer. This function is based on the ABC Engine functionality.
   For Bootstrapping the IDM includes a SAML IDP functionality. Hereby the password is a one time password, which is issued to the users for initial use. The IDM Portal does not have further sub-components, but is one application with interfaces to the the User Client (Web Browser) and IDM Application.

   The Interface to the User Client is compliant to HTML & HTTP including the standard SAML based interface toward service providers (e.g. the school or university registration system). To

learn about SAML please see e.g. Eve Maler's SAML tutorial [SAML]. As the portal does not have a database of the attributes of the user, the IDM application will be queried. The Privacy-ABC credentials issued by the IDM portal are stored by the user and used to create tokens, which are transferred to the service, eg. Student evaluation system or restricted area system, but no direct communication interface exists between Service Provider and IDM Application.

3. **The IDM Application** is the application that supports bootstrapping of the whole pilot. It may interface with other IDM systems, such as the university database, governmental or reputation services in the internet. Using the IDM portal relevant information is provided into the pilot and allows the user to edit his personal-non-anonymous data. While the data stored in the IDM application is non-anonymous and non-pseudonymous data. Additionally the IDM Application can read and verify Attribute tokens provided by the user. Please note while using the IDM application the users may not be anonymous. For a diagram of the IDM application, please see Figure 13.

   Two main components exist in the IDM Application, the SAML IDP and the ABC4Trust verifier. The SAML IDP works according to the SAML specification. It may provide an authentication of the user based on of several "out of bound" authentication methods. In the ABC4Trust pilots only OTP and ABC4Trust Token authentication will be used. The IDM Application has no own web browser interface as such, users will not "visit the IDM application" without being specifically redirected by a service provider to it. Then the only interface that might be shown in a web browser is a username/One Time Password login screen. The IDM Application will store the information, or get ABC Tokens by the user. The information will be evaluated, verified and a SAML reply will be given.

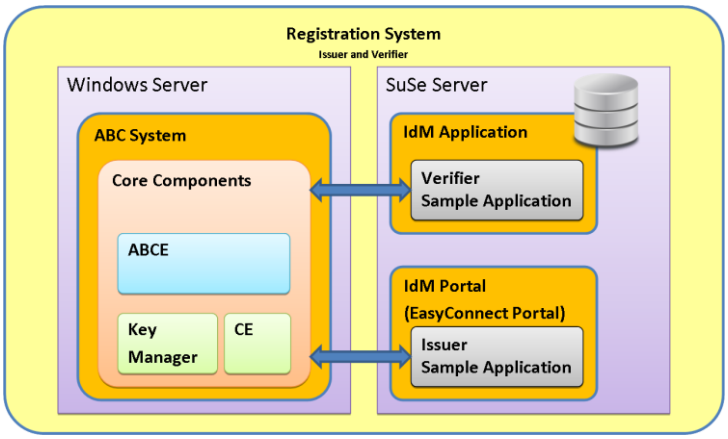

Figure 13: IDM Portal and IDM Application Architecture

3.1.2 Course Evaluation System

This component is responsible for the realization of the anonymous course evaluation process. Its sub-components are an ABC System and a Course Evaluation Application.

The ABC System is a component that performs access control to the Course Evaluation Application. This access control is achieved by presenting a policy to the potential users. Only users, who own credentials (e.g. course credential) that can be used to satisfy the access policy, are able to access the Course Evaluation Application.

The main component of the course evaluation system is the Course Evaluation Application.

The Course Evaluation Application is a web application that implements the functionality of the course evaluation procedure. Potential users of this application are students, professors and Hellenic Quality Assurance Agency (HQAA) members. Hellenic Quality Assurance Agency is the legal authority that supervises any evaluation procedure in Greek Universities. In particular:

- Course professors have the possibility to upload questionnaires regarding their course and determine the threshold number of attended lectures required for participating in the evaluation. This activity does not require ABC technology.
- Students are able to evaluate courses that they have registered to and attended
- When the evaluation procedure is completed, CTI members will collect and process the evaluation results in order to provide accumulated course evaluation results to HQAA. This off-line activity does not require ABC technology.

The Course Evaluation Application can be accessed only by users that own credentials that can satisfy certain policies. The application's access control functionality will be implemented by the Course Evaluation ABC system. This ABC system will only allow professors, certified students and HQAA employees to use this application. It will support role-based access and different actions will be allowed to each role. For instance, it will allow a professor to upload the questionnaires for his course, or it will allow certified students to fill in the available questionnaires. Each student is allowed to evaluate multiple times but only the last evaluation will be taken into account.

The Course Evaluation Application consists of a database that stores course information, the evaluation questionnaires, the answers from the students and other data related to the evaluation procedure.

3.1.3 Class Attendance System

The Class Attendance System is a system located in the lecture room of the University and it is responsible for providing attendance data to the students that participate in the pilot. More specifically, when a student attends a course lecture, she can wave her smart card in front of the Class Attendance System and obtain data on it. These data can later be used in order to prove that she actually attended the specific course lecture.

The Class Attendance System consists of a laptop and an NFC reader attached to it. The NFC reader is able to communicate with the contactless smart-cards that the students have. The Class Attendance System will be placed in lecture room 15 minutes before the start of the lecture and will be available for 30 minutes starting from 15 minutes before the end of the lecture. The Professor is responsible for fixing the exact times when each lecture of the course is happening (location, date, start and finish time). CTI in cooperation with PhD students will be responsible for the Class Attendance System's operation and physical security.

It consists of an ABC System and a Class Attendance Application. The Class Attendance Application runs on the laptop and is responsible for transferring (through the NFC reader) to the students' smart cards the attendance data related to specific course lectures. The ABC System will be used to issue attendance credentials to students with respect to their matriculation number.

The Class Attendance Application is a PC application responsible for storing attendance information on the students' smart cards. It will be executed on a laptop that is connected with an NFC reader that is able to communicate with the students' contactless smart cards. A PhD student is responsible for placing the laptop in the course lecture room before the lecture begins and configuring it according to the specific lecture.

The Class Attendance Application needs to be configured prior to each course lecture with the course identifier and the lecture identifier. This configuration will be done by CTI engineers. The Class

Attendance Application interfaces with the Class Attendance ABC System that is responsible for issuing attendance credentials with respect to the blinded student matriculation number.

3.1.4 User

This component refers to the interactions of the user with her smart card. The user has to install a software component on her PC. Its main sub-component is an ABC System. This software component is triggered every time a user is required to provide data stored on her card and asks for her consent. The equipment that is required for this component is a smart card reader. The ABC System provides to the user an interface between the browser and her smart card. For this reason, it employs a software component called "User Agent" that runs locally on her PC.

Moreover the Users can be informed about the system's functionality and can be instructed on how to operate it though Patras Portal.

Patras Portal: This component is an information web portal. Through this portal, the Users can be informed about the Course Evaluation for certified students. Thus, this page provides to the users the necessary links to the components of the system (e.g. University Registration System, Course Evaluation System) that are responsible for specific functionalities. Every time a user desires to interact with the system, her first action is to visit this portal and by following the instructions she can perform various pilot operations (e.g. register to a course, evaluate a course).

4 Scheduling of the Pilot, Detailed Project Plan

In this section we present the timeline of the scheduled tasks, deliverables, actions and deployments for realizing course evaluation for certified students.

4.1 Timeline

Starting from February 2012, the following take place:

- A student group consisting of 25 students is selected.
- The selected students are briefed on the scope and the goal of the pilot (ABC4Trust related information material will be distributed to them).
- Short seminars are organized in order to familiarize the students with the theory of digital credentials and the basic actions required for the testing. The user manual (appeared in Appendix C) will be ready. The user manual will be distributed to participated students in order to acquaint them with the pilot and its goals. Thus CTI will distribute in October 2012 and February 2013 the user manual to the two distinct groups of students.
- Students are educated into ABC4Trust concepts as well as pilot requirements. They will also be introduced to sample user interfaces so as to have early feedback to WP5.

As shown in Figure 14, by the end of February 2012, Deliverable D7.1: "Application Description for students" is available for review.

Between the beginning of March 2012 and the end of May 2012, the reference implementation from WP4 will be finished (see Figure 15). The WP5/WP7 system will be developed in parallel in close collaboration with WP4.

In May 2012, the Deliverable D5.2: "Description of the common denominator elements" will be available.

In May 2012, a preliminary on-site testing of early versions of the pilot system with a few students equipped with experimental smart cards will take place.

In August 2012, the Pilot system will be ready (with programmed smart cards delivered by WP4).

In September 2012, the final testing and debugging of the pilot system will be performed, leading to a final pilot system (deliverable D7.2, see Figure 14).

As shown in Figure 15, from the beginning of October 2012 to the end of January 2013 the First Round of the Course Evaluation Pilot will take place: students obtain ABCs, attend weekly classes, and attendance information is recorded on their smart cards. This lasts 13 weeks (in the meantime feedback is given, continuously to ABC4Trust consortium for improvements and correction of the architecture/reference implementation). In particular the following take place:

- University Enrolment: student registers at the university with his physical presence at the university's registration office. He gives informed consent on what data will be kept before any content is provided to.
- Department Registration: A student registers at the department's registration office.
- Course Selection and Registration: Students log on to on-line system in order to register and book a course.

- Attending Classes: attendance information in the first round of the Course Evaluation Pilot is updated by using a counter inside the smart card. In particular, this counter is increased when the students wave their smart card in front of the NFC after each class.

In the first week of February 2013 the actual evaluation of the courses takes place, while feedback is given to WP4 for preparation for the second round of the pilot (mid February 2013 to June 2013).

- Between February 2013 and June 2013 the Second Round of the Course Evaluation Pilot will take place (see Figure 15). The second group consisting of 25 students is selected. The timeline will be similar to the First round. However, the Second Round of the Course Evaluation Pilot will include the following additional features:
- Backup and revocation: Back-up is made locally on student's private PC (in order to recover from cases where a student loses his card).
- A full credential implementation will be used for the attendance data instead of the counter approach of the First round. Students will be issued attendance credentials. For this round of evaluation, the Class Attendance Application will be interfacing with the Class Attendance ABC System that will be responsible for credential issuance. The communication with the smart cards will be through the NFC reader. For this round of evaluation, parts of the cryptographic libraries are required to be ported and able to execute on the student smart cards.
- The credentials will carry more attributes.

In October 2013, formal evaluation results will be available to the ABC4Trust consortium (deliverable D7.3, see Figure 14).

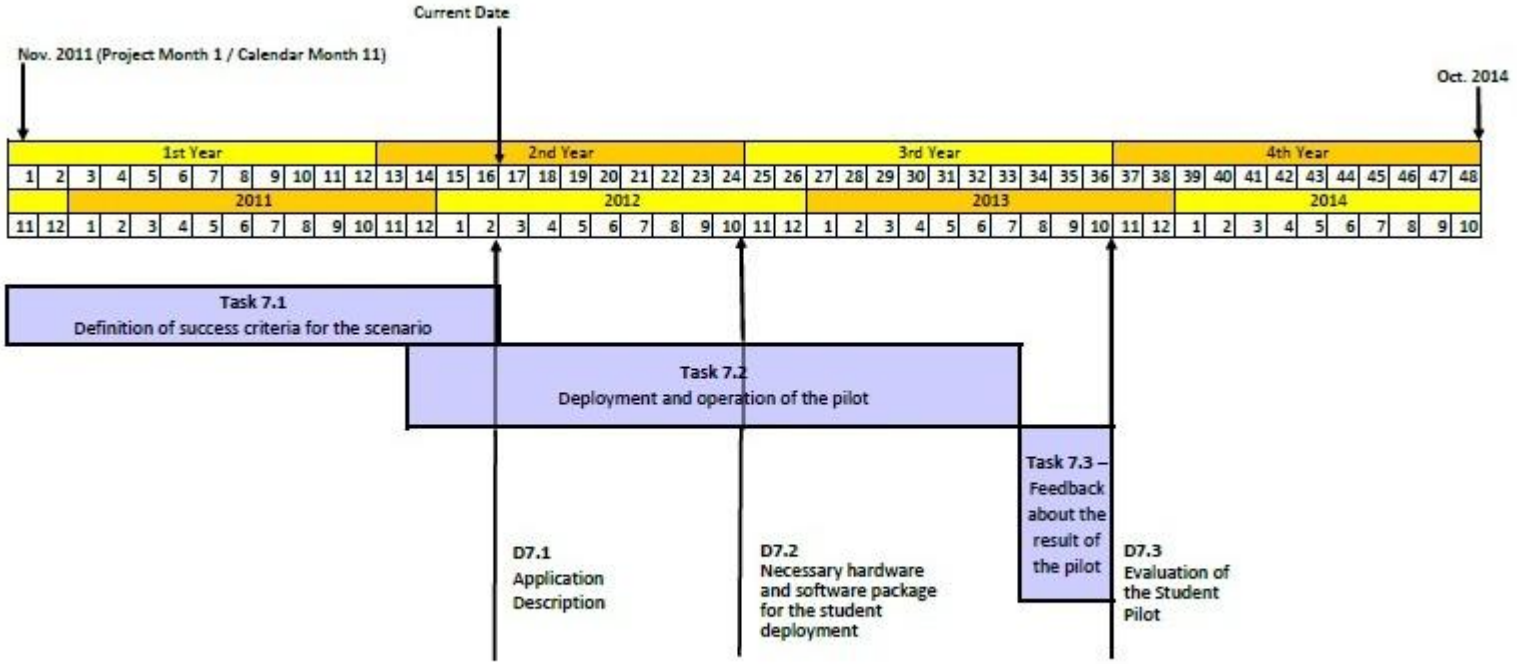

Figure 14: University Pilot Timeline

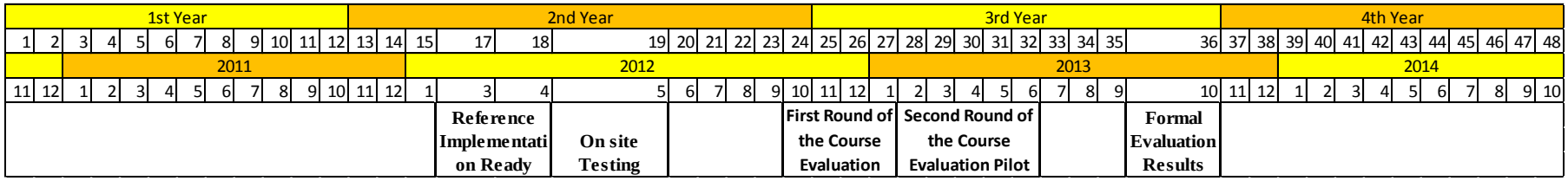

Figure 15: Course Evaluation Timeline

5 Requirements

In this section we provide a detailed description of requirements for the University Pilot. These include general system and academic requirements, privacy, security and assignment requirements. Finally, we discuss the availability, as well as volume and performance requirements for each part of the University Pilot System.

5.1 System Requirements

Participants in the pilot are:

- 25 students
- 3 professors and other university department personnel
- 3 CTI members

All usage of Users to Issuers and Verifiers will be through thin clients (web interface).

The administrator interface of the University Registration System (IdM) will be not http-based. Especially these administrator interfaces need to be protected from access via the internet.

5.2 Academic Requirements

- Students should be able to access, view, and edit their personal information stored in the system.
- Each student has to bring his smart card in the lecture room, in order to collect attendance information.
- Each professor has to specialise the course evaluation questionnaire.
- Class Attendance System will be placed in lecture room 15 minutes before the start of the lecture and will be available for 30 minutes starting from 15 minutes before the end of the lecture.
- The student has to wave his smart cart in front of a contactless NFC reader when leaving the lecturing room, in order to prove their attendance.
- Only students who have sufficient attendance may participate in the evaluation process.
- There are lower limits in the Course and Lab attendances: their individual values should exceed a threshold value.
- Each student must be able to evaluate a course multiple times but only the last one will be considered.
- HQAA will cooperate with the Department for the dissemination of the evaluation results
- There are lower limits in the Course and Lab attendances: their individual values should exceed a threshold value.
- Evaluations for different courses should not be linkable.
- If proof of a credential value implies revelation of identity, the student should be informed and give his/her consent to proceed with the evaluation.
- Evaluations for different courses must not be linkable.

5.3 Assignment Requirements

The planned assignments of University pilot have the following requirements:

- CTI must be responsible for the scheduling and realization of the Course Evaluation scenario.
- CTI must be responsible for the communication framework with Students, Professors and the Department of Computer Engineering and Informatics at University of Patras.
- Department's Registration Office employees have to provide a document containing a list of participating students together with department related data.
- Department's Registration Office employees have to provide students with a document which when signed guarantees their consent to participate in the pilot.
- Department's Registration Office employees will distribute to students a sealed envelope that contains secure hardware device (smart card) for storing his personal information and a PIN and a PUK for using it.
- Department's Registration Office employees will distribute smart card reader to each student.
- Department's Registration Office employees will distribute a one time password in order the students to be able to access the University Registration System for the first time.
- The department is responsible for distributing a general template of course evaluation questionnaire to the professors. The professor has to customize the course evaluation questionnaire to suit the course's needs.
- CTI will contribute to the deployment and operation of the Patras pilot. The systems required for the pilot will be placed at CTI premises.
- Department's lecture rooms must be accessible for the public.
- Department's premises are near CTI premises.
- CTI in cooperation with PhD students will be responsible for the Class Attendance System's operation and physical security.
- The University Registration System with will be placed at CTI's premises.
- The Course Evaluation System will be located at CTI's premises.
- CTI members must collect and process the evaluation results in order to provide accumulated course evaluation results to HQAA. HQAA have to disseminate the produced results to the department.

5.4 Availability Requirements

- University Registration System: The University Registration System should be available at all times, starting with the course semester. That is, students should be able to access it to view, edit or collect their ABC data at any time during the semester.

  This system should not go down. In case of malfunction (e.g. power failure), the System should come back and inform the student whenever it is back online (through ABC4Trust portal).
- The Class Attendance System should only be available for the duration of each course lecture and 15 minutes after the lecture. Typically, course lectures last two hours and there are two lectures per week.

This system should never go down during the course lecture. In case of malfunction, the system should recover in a couple of minutes. In order to increase Class Attendance System availability, there must be a second Class Attendance System in the lecture room.

- Course Evaluation System: The Course Evaluation System should be available for 5 weeks in total and mainly in evaluation period. In particular, it will be available for the last two weeks of the semester, in order for the professor to submit the course questionnaire. It will also be available for 2 weeks after the final exam of the course, in order for students to evaluate the course. During this time period the grades of the final exam will be known to all students. After the evaluation process has been completed, this system will be available for 1 week in order for CTI members to collect and process the evaluation results and provide accumulated course evaluation results to HQAA. This system should not go down during its availability period and mainly in evaluation period. In case of malfunction it should come back as soon as possible.

5.5 Defining Security and Data Protection Requirements with Protection Goals

In order to define the scope of the security and data protection aspects of the pilot, these aspects are briefly described in form of protection goals. We focus on the security as well as the data protection specific goals that should be achieved.

The security and data protection assessment continues as a necessarily ongoing task during the development of the pilot. In particular, further knowledge of the existing or planned implementation is necessary for identifying specific requirements to be derived from the applicable legal framework. So, once the development of the pilot commences, further details will be elaborated. By the launch of the test phase, a thorough documentation will be available as a project internal paper. Based on this documentation, a public description of the pilot, the data flows and the potential risks will be drafted and provided to the participants as part of the privacy policy.

The security related protection goals, as they have been discussed and accepted within literature (e.g. [FedPfi2000] can be summarised as follows:

Confidentiality: Confidentiality is the requirement that information is disclosed only to authorised users of a system. It is the most common security requirement in all information systems expected to be satisfied for both stored and communicated information.

Integrity: Integrity is the requirement that no unauthorised changes are made; both in data storage and in the transmission or that such change can at least be detected. For example, only authorised professors should be allowed to modify course material and grade.

Availability: Availability is the requirement that authorised users can use a system when needed. Therefore, it should not be possible for usage of the system to be maliciously denied. For example, the course attendance application should not need interaction to the IDM system.

To reach these goals, a series of security safeguards can be deployed for effective protection of the data. Examples for such security safeguards include:

- Encryption of data
- Data separation
- Transmission security
- An access authorisation concept

- Matching access controls
- Access log management
- Log files audit trail

As ABC4Trust being is a privacy oriented project, a focus alone on the security issues of the ABC technology implementation is not sufficient. This is caused by the fact that general data security aspects alone do not take into account the specific problems in relation to the processing of personal data, e.g. the data subjects rights. Therefore, further data protection related requirements need to be taken into account. To achieve this, the three established security protection goals confidentiality, integrity, and availability are extended by three additional data protection specific goals, which are unlinkability, intervenability, and transparency (for further details see [HSWH2011] [ZwiHan2012]).

These data protection specific protection goals are explained as below:

Unlinkability: "Unlinkability means that all data processing is operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy-relevant data outside of the domain, or at least that the implementation of such linking would require disproportionate efforts for the entity establishing such linkage. Unlinkability is the key element for data minimisation [PfiHan2010] because it encompasses all kinds of separating data from persons, e.g., by means of anonymisation, pseudonymisation, erasure or simply not having the data at all. In addition, it aims at separating different data sets, e.g., if they belong to different purposes, and thereby supports the principle of purpose binding. Further, separation of powers is related to unlinkability. Unlinkability in this wide definition comprises the criteria from the Privacy Class in the Common Criteria (anonymity, pseudonymity, unlinkability (in a stricter definition), and even unobservability in the sense that any observation of another party cannot be linked to the action or non-action of a user). The overarching objective of this protection goal is to minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling spanning across contexts and thus potentially violating the purpose limitations related to the data." (cited from [ZwiHan2012])

Transparency: "Transparency means that all parties involved in any privacy-relevant data processing can comprehend the legal, technical, and organisational conditions setting the scope for this processing – before, during and after the processing takes place. Examples for such a setting could be the comprehensibility of regulatory measures such as laws, contracts, or privacy policies, as well as the comprehensibility of used technologies, of organisational processes and responsibilities, of the data flow, data location, ways of transmission, further data recipients, and of potential risks to privacy. All these parties should know the risks and have sufficient information on potential countermeasures as well as on their usage and their limitations. This information should be given before the processing takes place (ex-ante transparency) which is in particular necessary if data subjects are being asked for consent or if data controllers want to decide on the usage of a specific system. But also subsequent to the processing, transparency on what exactly happened is important so that all parties can keep track of the actual processing (ex-post transparency)." (cited from [ZwiHan2012])

Intervenability: "Intervenability means that the parties involved in any privacy-relevant data processing, including the individual whose personal data are processed, have the possibility to intervene, where necessary. The objective is to offer corrective measures and counterbalances in processes. For individuals, intervenability comprises the data subject's rights to rectification and erasure or the right to file a claim or to raise a dispute in order to achieve remedy when undesired effects have occurred. For data controllers, intervenability allows them to have efficient means to control their data processors as well as the respective IT systems to prevent undesired effects. Examples for such means may be the ability to stop a running process to avoid further harm or

> allow investigation, to ensure secure erasure of data including data items stored on backup media, and manually overruling of automated decisions or applying breaking glass policies." (cited from [ZwiHan2012])

Together with the security goals, these form a set of overall six protection goals. This set can be used to frame conditions and map technical and organisational measures to use case scenarios. However, as these individual protection goals do complement each other, they also may stand in conflict with each other sometimes. In such event, a use-case oriented balance between individual conflicting goals must be found. The decisive factor for the balancing is a evaluation of the particular necessity of the protection goal for the use case [HSWH2011] [ZwiHan2012].

By applying these protection goals to the pilot as it has been documented by now, a series of legal and other requirements have been derived. These are shown in the next subsection.

5.6 Data Protection and Data Security Related Requirements

This section lists the data protection and data security related requirements that have been identified for this pilot. It contains generic requirements valid for most of the use cases. More specialised and use case specific requirements will then provide a comprehensive overview. The whole section 5.4 is subject to minor changes and amendments, as new challenges may be identified in the course of the further development of the pilot.

5.6.1 Generic Data Protection Requirements for the Pilot

This section briefly presents the generic requirements for effective and legally compliant data protection within the Patras pilot. It will convey two essential elements: First, we introduce some fundamental criteria for the lawfulness for processing of personal data in the European Union, respectively under the Greek transformation of Directive 95/46/EC. Second, additional generic data protection requirements that apply for the Patras University pilot are listed.

5.6.1.1 Generic Criteria for the Lawfulness of Personal Data Processing

The EU Data Protection Directive 95/46/EC is the main legislative framework regarding the processing of personal data for all member states of the European Union. Since the processing of the student's personal data is done by an entity seated in Greece (namely ABC4Trust partner CTI), the National law of this country is applicable. In Greece Directive has been implemented by Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data.[1] Hereinafter, we will refer to this law to derive some generic criteria for the lawfulness of personal data processing. These criteria are: Consent or other legal ground, predetermination for specific purposes/data minimisation, appropriate security safeguards and effective enforcement of the data subject's rights.

These criteria will be briefly explained to provide an overview of the frame conditions that apply for the processing of personal data under the scope of the Greek data protection law and Directive 95/46/EC respectively. In general a legal ground for the processing operation is required. The processing will be based on the informed consent of the person to whom the personal data relates (data subject). The granting of consent, however, must follow certain preconditions to be legally valid. Article 2(k) of the Greek Law 2472/1997 determines:

> *"The Data Subject's Consent" shall mean any freely given, explicit and specific indication of will, whereby the data subject expressly and fully cognisant signifies his/her informed agreement to personal data relating to him being processed. 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*

[1] Online http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL

recipients of personal data as well as the name, trade name and address of the Controller and his/her representative, if any. Such consent may be revoked at any time without retroactive effect."

To meet these requirements, it is necessary that the data subject is able to give consent:

- informed, i.e. with full knowledge about the purpose and conditions of the processing,
- freely, with full decision power and no serious disadvantages when consent is withheld,
- unambiguous, meaning without doubt about the expression of agreement,
- specific, i.e. related to a clearly specified purpose and processing operation.

These identified preconditions will be picked up as part of particular requirements below.

5.6.1.2 Particular Criteria for the University Pilot within ABC4Trust

The goal of the ABC4Trust project is showing the advantages of Privacy-ABCs as method for anonymous but secure and trustworthy authentication. From the view of the data protection law, Privacy-ABCs have a number of central advantages that are of relevance here (see [Kro11], p. 70 et seq.): First, Privacy-ABCs allow authenticating only with the attributes that are actually necessary to be processed for the purpose pursued by the data controller (selective disclosure). Second, if Privacy-ABCs are used to authenticate towards different services or for several access attempts, such actions remain unlinkable among each other, unless linkability is expressly required. Third, Privacy-ABCs further allow verifying that several credentials containing required attributes belong to the same entity without necessarily identifying this entity. To preserve these advantages, the following requirements should be fulfilled throughout the pilot:

- Methods for tracking or identifying Users such as IP logging, use of cookies or traffic analysis must not be used. In course of a pilot within a research project such as ABC4Trust, it might not be possible to address all such potential threats. In this case, the users should be pointed to existing solutions, e.g. for anonymizing IP-addresses users could be pointed to the existing onion routing services.[2] Ideally, the pilot deploys some safeguards on the network communication layer to secure Users from traffic analysis, IP logging, etc.
- Authentication must be possible with the necessary attributes only (selective disclosure).
- Users must be enabled to ensure that no more personal data than required to prove their access rights will be disclosed to the system. For this, Users require a general knowledge of the purpose of the processing and the personal data collected by the data controller for the named purpose.
- It must be possible to verify that several Privacy-ABCs belong to one entity without giving away identifying information, e.g. verifying that the credentials a particular value such as a User secret or the User's name without revealing this value.
- It must be possible for Verifiers to see whether a credential has truly been issued by a particular issuer.
- To prevent impersonation, the system must be capable of preventing access with lost smart cards or compromised credentials once a notification has been given, e.g., by revoking credentials.

The project's pilot deploying Privacy-ABCs must be legally compliant with data protection law and other applicable national legislation.

- Data subject's rights, such as the right of access and rectification, must be granted.

[2] For example, the TOR project with various free services, https://www.torproject.org/, or commercial service providers with a higher service level and speed such as e.g. JohnDonym http://anonymous-proxy-servers.net/.

- Personal data must only be accessible for authorized entities. Unusual access and processing should be made known to the data subject.
- According to the transparency principles, the User should be informed about who is processing which personal data for which purposes. Privacy-ABCs can be a major enabler for transparency as the GUI necessarily consists of a screen for attribute selection where the User can assemble the data to be sent. Also the necessary information about the receiving party can be displayed.
- Transparency requirements must be met, meaning that participants are enabled to learn to know who processes which personal data for which purpose. Possible measures to reach this goal include documentation, e.g., with:
    - Privacy and security policy including a description of the personal data processed and the purposes, the identity of the responsible data controller and involved data processors,
    - Description of the architecture and the data flows,
    - Contact details of the helpdesk or other persons than can help with problems,
    - Contact details for the revocation authority.
- For all data processed or stored, a clear and unambiguous deletion period must be specified depending on the type of data and purposes.
    - For the Patras University trial the IdM database must be deleted at latest one month after the official deadline end of the polling period(s).
    - The anonymous content of the polls and aggregated reports may be stored and processed for a longer period of time. However, as this information is personal information of the lecturer, some period should be stipulated in accordance to the necessities of the HQAA.
- Prior to the trail, the data retention periods will be fixed and communicated as part of the privacy policy.
- Personal data must not leave the smart card without the knowledge and consent of the user, e.g. the card could be secured with a PIN.
- The secret key stored in the smart card must not leave the smart card and the end user should be involved in the key generation phase.

Special regard must be given to the specialities of the Patras University trial. Object of the trial is the polling of students about the performance of a teacher / lecturer. In consequence similar requirements apply as to other types of votes or polls where manipulation should be impossible.

- Poll results must not be linkable to a particular participant.
- Evaluation must only be possible for participants that can verify to be students of the University and (regular) attendees of the particular lecture to be evaluated.
- The Evaluation may be done online. As a secure environment is absent (e.g. with a voting booth and personnel guaranteeing that only one person at the time enters) it must be prevented that participants are forced into giving particular results. Therefore it should be possible to change own votes until the final deadline of the poll. The necessary linkability with previous evaluation data must not result in the linkability of particular results to a person.
- It must not be possible to (self) create a valid credential.

5.6.2 Use Case Specific Data Protection Requirements

Several requirements are specific to use cases and will be discussed in relation to the respective use case. For details on the use cases, please refer to section 2.1 ("ABC system setup") above.

5.6.2.1 ABC System Setup

The following requirements regard the general setup of the ABC-system and of the necessary infrastructure such as the IdM application as part of the University Registration System.

- For processing personal data in a legal basis in form of an informed consent is required. During the setup phase this must cover in particular:
    - Transfer of student's and lecturer's personal data from Patras University's Department Registration Office to CTI as responsible data controller for the pilot,
    - Processing in the IdM system with CTI as data controller,
    - Processing of personal data during the issuing process,
    - Any processing of personal data during the evaluation phase.
- All participants must be informed about the modalities and circumstances of the data processing. This can be done e.g. with a privacy policy and/or a user's manual.
- The consent from the participants must be clear and unambiguous, freely given and specifically related to the processing operation in question to be valid in this trial.
- All the legal frame conditions have to be defined beforehand. This may encompass especially the legal basis for the personal data processing in its whole lifecycle (collection, processing, storage, deletion), such as the contract or permitting law. Moreover, the privacy policy is part of these legal frame conditions.
- Generally users must not be tracked with means such as cookies, IP-addresses, traffic analysis, etc. For access to the IdM system User's must be identified to get access to their personal data. Here it is acceptable to deploy session cookies to enhance data security.
- All secret keys must be kept confidential (User, Issuer, Revocation Authority).
- The User secret on the smart card must not leave the card. Only the user must be able to make use of it.
- The University Registration System including the IdM System must be secured against unauthorized access to personal data.
- It is possible for participants to leave the trial, e.g. by leaving University or revoking their consent. Their personal data will then be deleted from the IdM database and the User's credentials will be made invalid for course evaluation. Where necessary, a backup procedure for participating in the evaluation will be available (e.g. paper based within a group of students).
- The User must be given access right to the content of her Smart Card except the user Secret (this one is provided as a built-in feature by the Smart Card).
- If administrative tasks require access to personal data this access must be documented in log files. Plausibility checks regarding the necessity of the access will be done in regular intervals.
- Data processing (here from NSN on CTI systems) requires a written contract between the data controller and the data processors. Details such as technical and organisational measures to ensure data security and data protection must be internally documented.
- The IdM database is physically located in Patras, Greece. Remote access for administrators located at NSN in Munich must be possible.

- Access by data processors to the database with the participant's data should be traceable for the data controller. Plausibility checks regarding the necessity of the access will be done in regular intervals.
- Reasonable technical and organisational measures to protect personal data in the University Registration System must be taken. These will serve general data security as well as specifically personal data protection purposes. Generally, access to the personal data of test participants for NSN should be strictly limited to the extent absolutely necessary. During the further project runtime, organisational and technical measures will be identified in cooperation with all involved partners. Examples for such measures are:
    - Logging of remote accesses or automated messages to the responsible entity (school administration).
    - Preferably, the maintenance of the IdM system should take place without granting any access to participant data. Where such access is necessary, double-check procedures should be established, e.g., by having a local representative watch the access on-screen in real time.

5.6.2.2 Obtaining the University/Course Registration Credential

This section lists requirements related to obtaining a credUniv credential for the first time or for obtaining a new or updated credUniv using a valid credUniv already in the possession of the User.

- The user obtains a one-time-token that is known by the Student and the University only.
- This one-time-token must be valid, until the credUniv has been successfully issued. The student must be able to request a new one-time-token in case of electrical-, network- or hardware failure.
- The system should be accessible online for authorized Users.
- Issuance of a credential must be limited to the authorized User.
- Where possible students may correct false personal data either by rectifying the information themselves or by requesting such a rectification.
- It must not be possible to (self) create a valid credential proofing false information.
- The University Registration System (Issuer) must be sufficiently reliable during the roll out phase of the smart cards.
- Only authorized issuers must be able to issue a valid credential. In case of unauthorized issuers, this lack must be detectable for verifiers.

5.6.2.3 Obtaining Class Attendance Data

- Only authorized Issuers must be able to issue a valid credAttendance. In case of unauthorized Issuers, this lack must be detectable for verifiers.
- The system issuing the attendance credentials must not collect any identifying information from the students including the matriculation number.
- The smart card must not give away any personal or identifying information without consent of the user proven by PIN entry.
- Linkability between sessions must not be possible, in particular the smart card must not send any unique identifier (during handshake or issuance protocol) allowing to link different occasions of attendance.

- It must not be possible to reach the quantum of attendance with credentials collected during fewer lectures. E.g. prevent collecting more than one credential per lecture or prevent presentation of more than one credential for each lecture (cf. Use Case GR_9).
- The issuance system must be reliably available during the particular collection period for a lecture. An alternative process may be defined to substitute the system, e.g. with paper vouchers.
- An alternative process should also be available for lost or forgotten smart cards, e.g. with paper vouchers.
- What happens during the issuance process must be correctly documented and this documentation must be available to the Users.

5.6.2.4 Backup and Restore of Smart Card Content

- Users may backup and restore credentials and other smart card content locally on user-controlled systems.
- The backup data should be stored in an encrypted format.
- The User may not backup the user secret on the smart card.
- Users should be instructed to backup their credentials regularly.
- The setup should be accompanied by a detailed documentation of the system and the services provided including backup and restore, e.g. as part of a handbook.
- Changes to the personal data in the backup system must be detectable. The right to change data must be restricted to authorised persons.

5.6.2.5 Revoking a Student's Privacy-ABCs

The revocation process must be seen in context with potential reasons for a revocation. Besides the loss of a smart card these also include the e.g. cases of a participant leaving the university, unregistering for the class or withdrawing consent to the data processing in the ABC4Trust trial. Given these considerations the following requirements have been derived:

- Is there a predefined specific deletion period for personal data (e.g. at a certain time span after the end of the pilot) must be set.
- A procedure must be set up to prevent that a User gets impersonated or a credential can be used to authenticate towards the system after an incident requiring a revocation has been reported. This service needs to be available and react within an appropriate timeframe.
- Users will be informed about revocation reasons.
- Users know how to trigger a revocation process with the Revocation Authority in case of e.g. a lost smart card. For this the User must authenticate herself as authorized person concerned.
- If revocation is not followed by re-issuance of a new credential, e.g. as the student leaves the university or has withdrawn consent, the data in the IdM database must be deleted within due time (without remainders of data copies, e.g. from backups). If protocol and log files are necessary for legal/audit purposes these information may be processed only for purposes of ensuring IT security.
- The information that will be published to declare the revocation must not identify the user or contain unique identifiers.

5.6.2.6 Course Evaluation

- Poll results must not be linkable to a particular participant. Participants must not be identified.
- Evaluation must only be possible for participants that can verify to be students of the University and (regular) attendees of the particular lecture to be evaluated.
- It must not be possible to reach the quantum of attendance with credentials collected during fewer lectures. E.g. prevent collecting more than one credential per lector or prevent presentation of more than one credential for each lecture.
- Every participant may only contribute one valid poll questionnaire.
- Re-evaluating: The evaluation may be done online. As a secure environment is absent (e.g. with a booth and personnel guaranteeing that only one person at the time enters) it must be prevented that participants are forced into giving particular results. It should be possible to change own evaluations until the final deadline of the poll. The necessary linkability with previous evaluation data must not result in linkability to a particular person.
- A functional requirement demands that it should be possible for Users to redo an evaluation until the final polling deadline with only the last poll being valid. To enable this feature, it is acceptable to provide the User with a hook linking to the already existing results. However it must not be possible to link the stored result of a poll to a particular User without a contribution of the User.
- The participation in the trial must be based on valid, freely given consent of the students. This means that in case of students not wanting to participate in the trial, alternatives must be provided for. This entails participating in the e-voting without taking part in trial as well as choosing a paper-based voting. For the trial process itself, this means that precautionary measures must be taken to avoid a potential identification in case not all students of the classes can take part in the electronic poll. Thus, a minimum size of the anonymity set must be ensured for any group of participants in the evaluation. Whereas anonymity may be quite difficult to measure on a small scale, a possibility may be to assume a minimum set of 5-10 participating students, which may be enough to provide a sufficient level of anonymity for the evaluation of a lecturer. This results in the following requirements within the University trial:
    - Enable participants to withdraw consent and provide for a paper based evaluation during the trial by a control group. The evaluation within the trial must be done with a minimum size of members as otherwise the results would be easily linkable to the one or few members of such a group.
    - Results of the electronic poll must only be accessible if a minimum of votes has been submitted.
- Other methods to identify or track a User must not be used during the course evaluation.
- If cookies are necessary, they must be deleted after logout. In this case, the fact of setting a cookie must be transparent.
- It must not be possible to access submitted poll results before end of the polling period.
- It must not be possible to change submitted poll results by anyone but the User. Until the end of the polling Users are allowed to re-evaluate / change their particular evaluation.

5.6.2.7 Requirements Related to the Right of Access and Rectification

The participants have the data subject's right to access and rectification of personal data according to Art. 12 of Directive 95/46/EC. This is not only valid for personal data under the control of a third

person (IdM system, see above), but also for data under the physical control of the User herself, and thus applies to the data stored on the smartcards.

- The User must be given access rights to the content of her smart card.
- In case some data is excluded from access, this must be known to the user, e.g., the User's Secret as a feature provided by the Smart Card cannot be accessed for security reasons.
- The information must be displayed completely & correctly.
- Only the User may have viewing access.
- User must be able to administer own credentials e.g. deleting them from the smart card.
- Deletion of credentials on the smart card requires the User's confirmation, e.g. with PIN for access.
- The User must be granted their right of access to personal data stored in the IdM.
- Access of unauthorized persons to the content of the IdM System must be prevented, including the system administrator.
- Fine-grained access authorisation concepts to the administrative section of the IdM system are required, including matching access controls.
- In case some data is excluded from access, this must be known to the user, e.g., the User's Secret as a feature provided by the Smart Card cannot be accessed.
- Users must have the possibility to have false personal data in the IdM system and in their credentials rectified, e.g. by sending a request to the staff responsible for the University Registration System.

5.7 Volume and Performance Expectations

- University Registration System: Taking into account the number of users in the system, the latter should be able to handle 25 records per day.
    - System Setup: The average data transaction will be small because information about all of the 25 users participating in the pilot needs to be transferred to the system.
    - Registering: It is expected that the beginning of the course semester will be a peak processing period lasting 2-3 weeks. The average data transaction during the beginning of the course semester will be large. During this period, the data transmission will also be large because all the 25 students will be collecting their ABCs. During the semester, the data transactions will be small and not evenly distributed in time.
    - Self-administration: The average data transaction will be small and peak processing periods are not expected. The average data transmission will also be small.
- Class Attendance System: At the end of the course lecture will be a peak processing period.
- Course Evaluation System:
    - Questionnaire's submission: Whenever the professor uploads the questionnaire on the course evaluation system, tens of records will be transmitted and processed.
    - Voting: The week around the date of the final exam is expected to be a peak processing period. During this period, data transaction will be large. Course evaluation system has to transfer the questionnaire data to all users' browsers, thus data transmission is large.
    - Results: When results are to be disseminated, a few records will be published.

5.8 Required Attributes in the Credentials

In this pilot, three types of credentials will be used. The first one called "credUniv" is the credential that a student receives from the University Registration System when he registers as a student. It contains the following attributes:

Credential Name:	**credUniv**
Attributes:	First Name
	Last Name
	University Name
	Department Name
	Matriculation Number
	Revocation Handle

Table 10: University Credential

The next credential called "credCourse" is the credential that a student receives from the University Registration System when subscribing to a course. It contains the attributes:

Credential Name:	**credCourse**
Attributes:	Matriculation Number
	Course Identifier

Table 11: Course Credential

Finally, in the case we use credentials for the proof of attendance the credential called "credAttendance" will contain the following attributes:

Credential Name:	**credAttendance**
Attributes:	Matriculation Number
	Course Identifier
	Lecture Id:

Table 12: Attendance Credential

5.9 ABC Features Referred in D5.1

In this section we refer related information to the D7.1 deliverable that is found in the already submitted deliverable D5.1 [DSDBP12]. This information will complete the whole picture of the University Pilot. We refer to the following information:

- ABC Roles and Legal Roles: Section 2 in D5.1 discusses the roles of the pilot stakeholders with respect to the two ABC4Trust Pilots. There are two different types of roles:
    - ABC roles: These pertain to the ABC related functionalities and are presented in Section 2.1.
    - Legal roles: These pertain to the protection of personal information items of the pilot participants and are presented in Section 2.2.

- Detailed Description of Credentials: Sections 4.4.1 to 4.4.3 in D5.1 present in detail the different credentials that are being issued to a student during the deployment of the University Pilot. These are credUniv, credCourse and credAttendance.
- ABC Proofs: Section 4.4.4 in D5.1 provides an analytic description of how the University Pilot Credentails are used in order to certify a number of facts about the student (e.g. matriculation number, name, department, percentage of attendance of a course, etc.), allowing those with proper credentials to anonymously provide feedback on two courses and teachers they had during a semester.
- Data Flows: Section 4.5 in D5.1 provides a detailed description of the basic scenarios data flows between architecture entities. These take place when a student obtains the University/Course Registration Credential, when he obtains Class Attendance Data and also in the course evaluation.

6 Pilot Impact and First Feedback

In this section we introduce the impact of course evaluation for certified students in Greek community. Moreover in order to have a general overview of students and professors expectations for the course evaluation we tried to get a first feedback from them, which is presented in section 6.2.1and 6.3.1.

6.1 Pilot Impact in Greek Community

The Greek Schools' Network (GSN[3]) is the educational intranet of the Ministry of Education and Religious Affairs[4], which interlinks all schools and provides basic and advanced telematics' services. Thus, it contributes to the creation of a new generation of educational communities, which takes advantage of the new Informatics' and Communication Technologies in the educational procedure. Computer Technology Institute controls and monitors this network and its ambition is to introduce to it Privacy-ABC technologies.

The implementation of the Greek Schools' Network is funded by the Framework Programme for the Information Society[5], in close cooperation between the Ministry of Education as well as 12 Research Centers and Highest Education Institutes, specialized in network and Internet technologies.

The current design and implementation of the Greek Schools Network focuses in providing useful services to all members of the basic and middle education community, fulfilling among others the following goals:

- Access to telecommunication and informatics services
- Access to digitized educational material
- Distance learning, e-learning
- Encourage collaboration
- Information and opinion exchange
- Conduct of thematic discussions, seminars, lectures, etc.
- Access to digital library services
- Communication and Cooperation of all educational degrees
- Communication with European educa-tional networks
- Facilitate complimentary educational programs
- Provide education to individuals with special needs or disabilities
- Inform, educate, entertain

In order to maintain the educational orientation of the network, its users are certified individuals, educational or administrative entities of the National Education. In particular, the users are divided in the following categories:

[3] www.sch.gr
[4] www.ypepth.gr
[5] www.infosoc.gr

- **Schools:** At least one user account have been provided to all middle grade education schools and 92% of first degree education schools.
- **Administrative units:** At least one user account has been provided to more than 2.282 administrative units of National Education.
- **Educational staff:** The Greek Schools Network offers fully personalized access to all educational staff, with the dial-up service being broadly used under certain terms.
- **Students:** Network access is provided to students through the school laboratories. In addition, personalized access is offered to second grade students since September 2008.
- **Administrative staff:** as with educational staff.

The Greek Schools Network offers a broad package of services to its units and users. The most important of these are:

1. Automated registration procedure for educational staff and students - Users Administration Service
2. Remote network access (dialup)
3. Mail, accessible through the POP3 and IMAP protocols, as well as the world wide web www.sch.gr/mail
4. E-mail lists www.sch.gr/lists
5. Web Portal (www.sch.gr), offering news services and personalized access to telecommunication and informatics services
6. Controlled access to the World Wide Web, prohibiting access to web sites with harmful content for underage
7. Web hosting for static and dynamic pages
8. Wizards for automatic webpage creation
9. Asynchronous distance learning, for hosting and distributing digitized lessons (www.sch.gr/e-learning)
10. Teleconference www.sch.gr/conf
11. Video On Demand (www.sch.gr/vod), delivering streaming educational multimedia material
12. Live Internet transmission (webcasting) of various of various events (www.sch.gr/rts)
13. News (www.sch.gr/news) and Discussions (www.sch.gr/forums)
14. Electronic Magazine (www.sch.gr/magazine)
15. Personal Calendar, Personal Address Book, Notes and "To Do", accessible through the World Wide Web
16. Directory Service
17. GIS
18. Voice over IP
19. Online statistics (www.sch.gr/statistics)
20. Blogs (http://blogs.sch.gr)
21. Help-Desk, for immediate solution of technical problems.

We believe that a successful pilot at the University of Patras will provide sufficient proof of concept for the acceptance and the wider applicability of Privacy-ABCs throughout the Greek Schools Network. CTI controls this network, a fact that will facilitate the adoption of ABCs in the everyday lives' of members of the Greek educational community.

6.2 Feedback from the Students

It is important for the University Pilot's success to get feedback from students for the course evaluation. We have planned the distribution of questionnaires in which the opinion of the students will be collected and analysed with regard to several usage criteria of the anonymous credentials concept as well as the reference implementation.

We have to organize three distributions of questionnaires and to compare the produced results:

- The first questionnaires happen before the pilot's demonstration and before students are informed about ABC technologies. Here we will have questions about students' distrust on electronic evaluation systems and traditional evaluation procedure. Our first feedback from students and professors intent to adjust the University pilot according to the needs of the students and the professors.
- The second one after the first evaluation. Here we will have questions about students' knowledge on ABC technologies.
- The third one after the second round of course evaluation. Here we will have questions about students' experience on ABC technologies and evaluation.

6.2.1 Results from 1st Questionnaire

On 17/03/2011 in the beginning of a lecture, slides were shown introducing the students to the concepts of ABC Credentials and the goals of the pilot. On 18/03/2010 in the begging of their lecture, the introduction about ABC technologies was concluded and a discussion related to the concepts of ABC Credentials, the conductance and the goals of the pilot, was held. For further and more detailed information on the course evaluation pilot, students were referred to the Pilot's Greek site.

We distributed hard copies of the questionnaires to 71 Students in class and all of them filled the questionnaire. The format of the distributed questionnaire to students is appeared in Appendix A.1.1. A subset of those students will actively participate in the course evaluation pilot. In general students found the course evaluation pilot quite appealing as you can see from Figure 16 and Figure 19. Students found ABC Technologies interesting (see Figure 17 and Figure 23) and they believed that it can change their everyday life (see Figure 24). Although their trust level for previous evaluation methods was good (see Figure 22), their trust level for the anonymous evaluation process was even higher. Moreover, students were asked about which attendance process they preferred (see Figure 25--Figure 29) and found the first method more trustful, efficient and easy to employ. Their main concern was on the impact that the results of the evaluation process will have on the conductance of the course (see Figure 30--Figure 33). .Finally, a demo of the evaluation pilot could increase students' trust level as shown in Figure 21.

6.3 Feedback from the Professors

6.3.1 Results from 1st Questionnaire

We sent to 14 professors and lecturers by mail the questionnaires and all of them filled the questionnaire. The format of the questionnaire is appeared in Appendix A.2.1. The email included a brief introduction to the concepts of ABC credentials and the goals of the pilot and for further and more detailed information on the course evaluation pilot professors were referred to the Pilot's Greek site.

In general professors found the course evaluation pilot quite appealing and they found ABC Technologies interesting (see Figure 35 and Figure 38). Professors believe that anonymous credential systems can change their everyday life (see Figure 48). Although their trust level for previous evaluation methods is good (see Figure 39), 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 (see Figure 40--Figure 43). Their main concern is on the impact that the results of the evaluation process will have on the course improvement (see Figure 37). Finally, most of the professors believe that the evaluation results should be accessible from University's personnel (see Figure 44).

7 Bibliography

[ABC11] Project Description, ABC4Trust-Attribute-based Credentials for Trust

https://abc4trust.eu/

[Art29WP160] Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General guidelines and the special case of schools), adopted on 11 February 2009, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009_en.htm

[DSDBP12] Souheil Bcheri, Norbert Götze, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Yannis Stamatiou, Katalin Storf, Peder Wängmark, Harald Zwingelberg. D5.1 Scenario definition for both pilots, 2012, https://abc4trust.eu/index.php/pub/

[BCGS09] Patrik Bichsel, Jan Camenisch, Thomas Groß, and Victor Shoup. Anonymous credentials on a standard java card. In Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, pages 600–610, New York, NY, USA, 2009. ACM.

[BDDD07] Stefan Brands, Liesje Demuynck, and Bart De Decker. A practical system for globally revoking the unlinkable pseudonyms of unknown users. In Proceedings of the 12th Australasian Conference on Information Security and Privacy, ACISP'07, pages 400–415, Berlin, Heidelberg, 2007. Springer-Verlag.

[Bra93] Stefan Brands. Untraceable off-line cash in wallets with observers (extended abstract). In CRYPTO, pages 302–318, 1993.

[Cam06] Jan Camenisch. Protecting (anonymous) credentials with the trusted computing group's TPM v1.2. In SEC, pages 135–147, 2006.

[CCS08] Jan Camenisch, Rafik Chaabouni, and Abhi Shelat. Efficient protocols for set membership and range proofs. In ASIACRYPT, pages 234–252, 2008.

[CG08] Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. In ACM Conference on Computer and Communications Security, pages 345–356, 2008.

[CHK+06] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to win the clone wars: efficient periodic n-times anonymous authentication. In ACM Conference on Computer and Communications Security, pages 201–210, 2006.

[CHL06] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Balancing accountability and privacy using e-cash (extended abstract). In SCN, pages 141–155, 2006.

[CKS09] Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In Public Key Cryptography, pages 481–500, 2009.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In EUROCRYPT, pages 93–118, 2001.

[CL02] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to

efficient revocation of anonymous credentials. In CRYPTO, pages 61–76, 2002.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In CRYPTO, pages 56–72, 2004.

[CS03] Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In CRYPTO, pages 126–144, 2003.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. Commun. ACM, Vol. 28, No. 10, pages 1030–1044, 1985.

[FedPfi2000] H. Federrath,,A. Pfitzmann, Gliederung und Systematisierung von Schutzzielen in IT-Systemen, Datenschutz und Datensicherheit (DuD), Vol. 24, No. 12, pages 704–710, 2000.

[HSWH2011] H. Hedbom, J. Schallaböck., R. Wenning, M. Hansen, Contributions to Standardisation. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.), Privacy and Identity Management for Life, pages. 479–492, 2011. Springer, Berlin.

[Kro11] I. Krontiris (Edr). D2.1 Architecture for Attribute-based Credential Technologies – Version 1, 2011 https://abc4trust.eu/index.php/pub/107-d21architecturev1

[PfiHan2010] A. Pfitzmann, M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, 2010,

http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[ZwiHan2012] H. Zwingelberg, M. Hansen. Privacy Protection Goals and their Implications for eID System. In Simone Fischer-Hübner, et al. (Eds). Proceedings of the IFIP Summer School 2011, Springer Boston, to appear 2012.

[OASIS] S. Cantor et al., Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005. Document ID saml-core-2.0-os http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML] Eve Maler. SAML basics - A technical introduction to the security assertion markup language, http://www.itu.int/itudoc/itu-t/com17/tutorial/85573.html.

[Ngu05] Lan Nguyen. Accumulators from bilinear pairings and applications. In CT-RSA, pages 275–292, 2005.

Appendix A Questionnaires

A.1 Student Questionnaire

A.1.1 Questionnaire Format

ABC4Trust Acceptance Questionnaire for Students

Rating Instructions:

Please answer the questions regarding the following rating scores:

Score	1	2	3	4
Level	Poor	Fair	Good	Excellent
Agreement	not at all	partially	mostly	fully
Acceptance	No			Yes
Importance	not important	somewhat important	important	extremely important

Questionnaire:

Question / Rating	1	2	3	4	5
1. Is it important for you to maintain your anonymity when participating in a course evaluation? (Hint: use the agreement rating)					
2. Do you trust more an electronic evaluation system than an administrative organization to implement the evaluation of a course?					
3. Do you believe that it is easier to maintain your anonymity by a secure electronic system?					
4. If you were sure that the evaluation process maintains your anonymity, would you answer differently to the provided questionnaire?					
5. Can a reliable and trusted evaluation system collect data that will improve the process of the course?					

6. Could a live demonstration of an electronic evaluation system increase your trust on evaluation process? (Hint: use the agreement rating)	

Question / Rating	1	2	3	4	5
7. What is your trust level to the course evaluation based on previously applied methods (e.g. paper-based surveys) ? (Hint: use the level rating)					
8. Are you already aware of the credentials' terminology?					

Regarding course attendance two methods are proposed:

First Method: A student waves his student card over a smart card reader so that "attendance information" is issued to his card.

Second Method: One-time codes are distributed to a student on paper during lecture. At home, he/she enters these codes in a website which issues the "attendance information" to his student card. In order to have access to the website, he will use a piece of software distributed by the University. After using this code once, the same code will not be accepted by the website any more.

Question	Method 1	Method 2
9. Which of the proposed methods would you prefer regarding trustfulness?		
10. Which of the proposed methods would you prefer regarding ease of use?		
11. Which of the proposed methods would you prefer regarding efficiency?		

Question / Rating	1	2	3	4	5
12. Regarding the **First Method** do you prefer to receive a 'proof' (e.g. a beep) that the transfer of the attendance information to your smart card was successful? (Hint: use the agreement rating)					
13. Regarding the **Second Method** do you believe that these codes will be forwarded by the professors to non-present students in order to get a higher percentage of course attendance in the statistics? (Hint: use the agreement rating)					

14. Please rate the importance of the following course poll goals, according to the rate table. (Hint: use the importance rating). If you have any other suggestion, please write it.	1	2	3	4	5
➢ Providing feedback to the lecturer so that the quality of the course is improved					
➢ Evaluating the qualities of the professor					
➢ Refining the curriculum (e.g. delete unattractive courses)					
➢ Your suggestion:					

Please check only one answer to the following questions according your opinion. If you have any other suggestion, please write it.

15. Who should be able to read the results of a course evaluation?	
➢ Everyone (public results)	
➢ Personnel of the University including all students and all professors	
➢ Only students who attend the course and the corresponding professor ➢ Your suggestion:	

Question / Rating	1	2	3	4	5
16. Could the concept of digital credentials be applied to other aspects of your life?					

A.1.2 Results

1. Is it important for you to maintain your anonymity when participating in a course evaluation? (Hint: use the agreement rating)

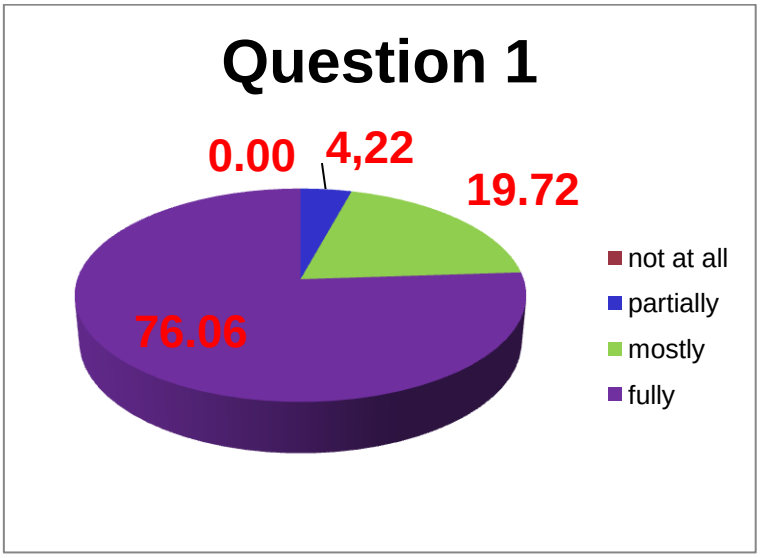

Figure 16: Result of Question 1 in Students Questionnaire

2. Do you trust more an electronic evaluation system than an administrative organization to implement the evaluation of a course?

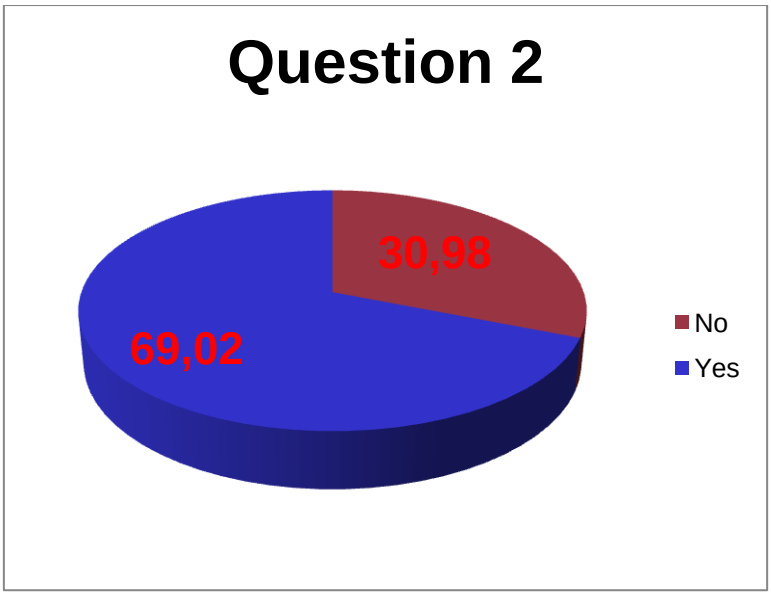

Figure 17: Result of Question 2 in Students Questionnaire

3. Do you believe that it is easier to maintain your anonymity by a secure electronic system?

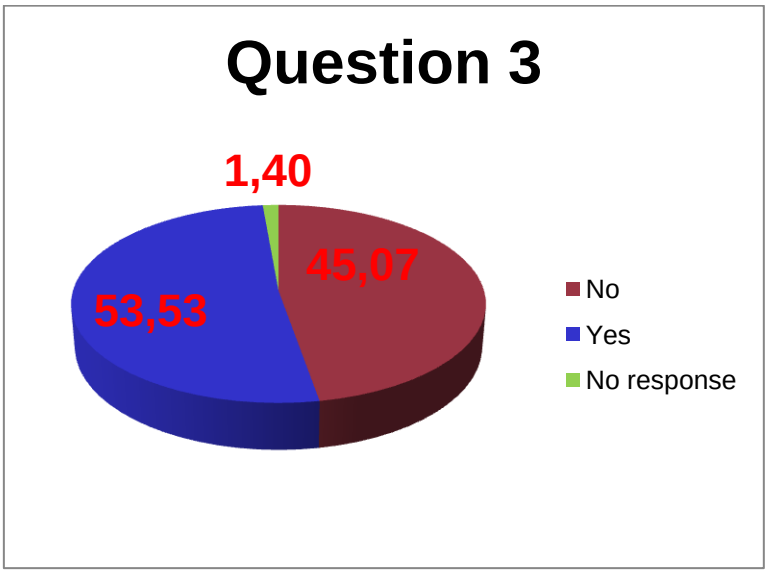

Figure 18: Result of Question 3 in Students Questionnaire

4. If you were sure that the evaluation process maintains your anonymity, would you answer differently to the provided questionnaire?

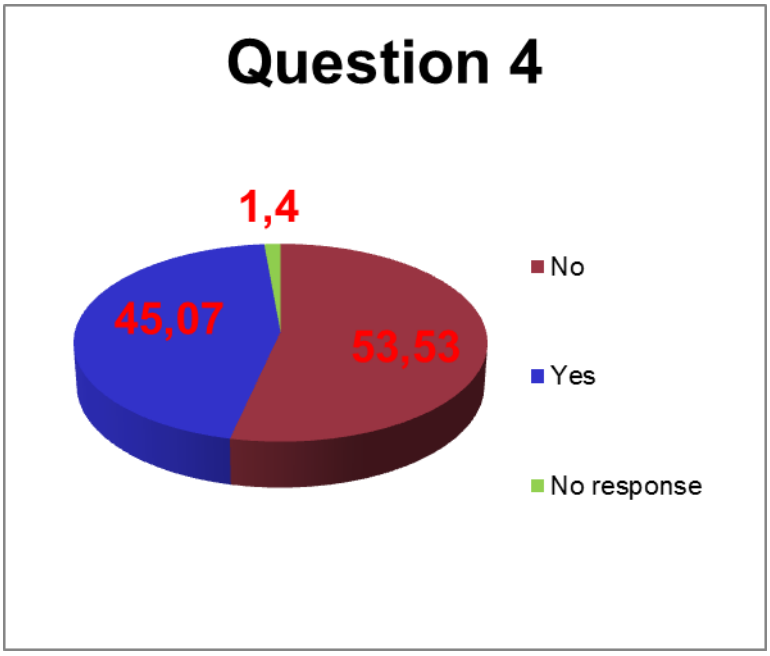

Figure 19: Result of Question 4 in Students Questionnaire

5. Can a reliable and trusted evaluation system collect data that will improve the process of the course?

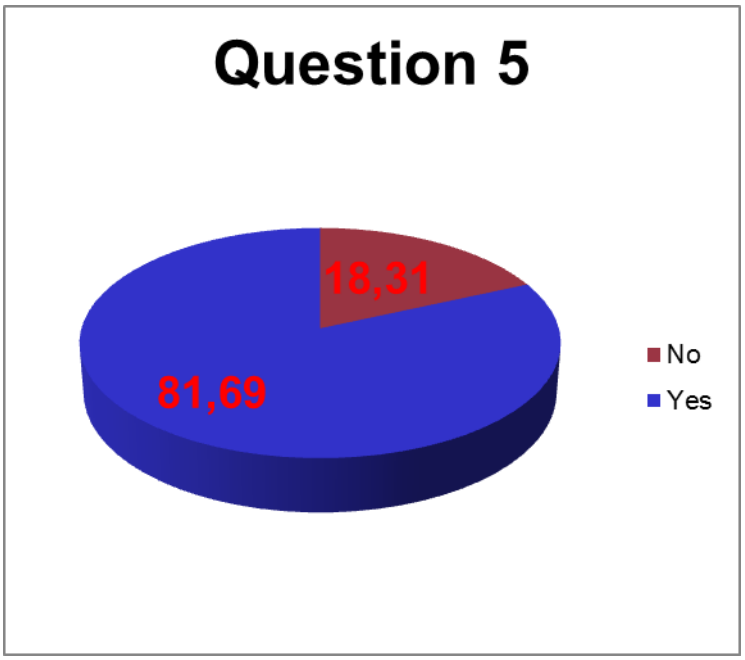

Figure 20: Result of Question 5 in Students Questionnaire

6. Could a live demonstration of an electronic evaluation system increase your trust on evaluation process? (Hint: use the agreement rating)

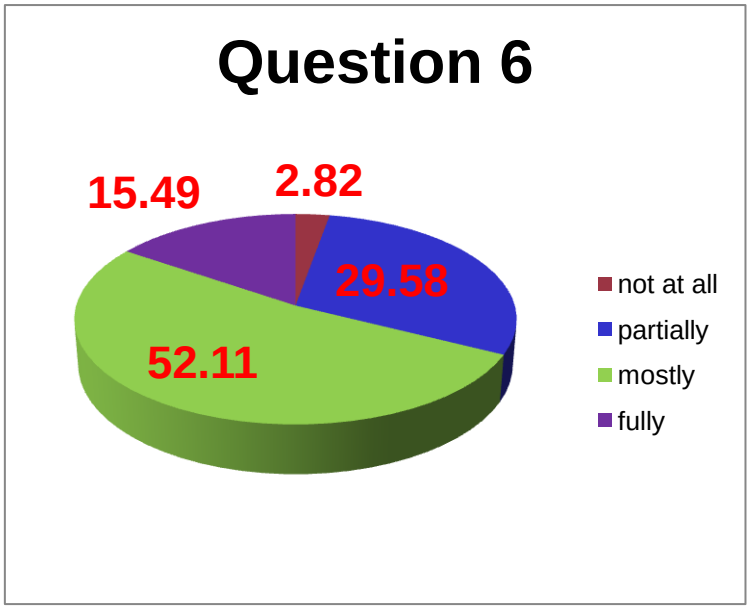

Figure 21: Result of Question 6 in Students Questionnaire

7. What is your trust level to the course evaluation based on previously applied methods (e.g. paper-based surveys) ?

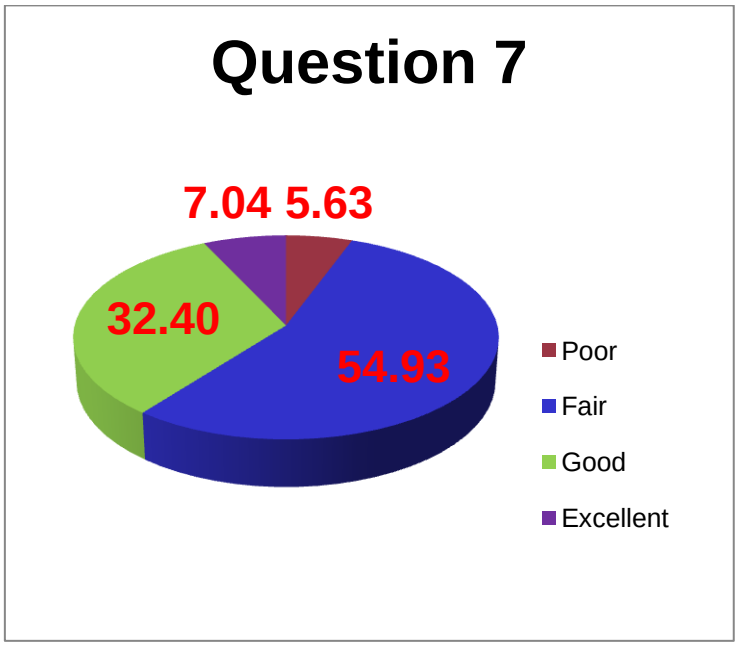

Figure 22: Result of Question 7 in Students Questionnaire

8. Are you already aware of the credentials' terminology?

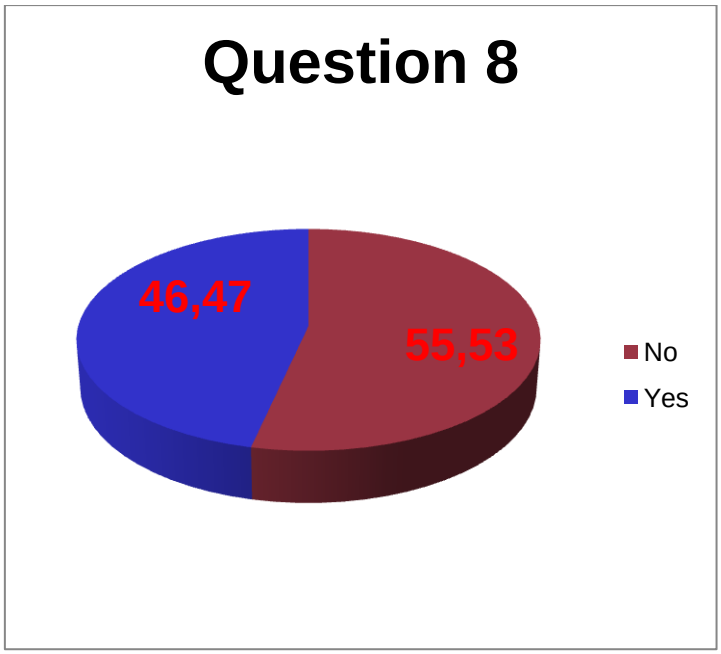

Figure 23: Result of Question 8 in Students Questionnaire

9. Could the concept of digital credentials be applied to other aspects of your life?

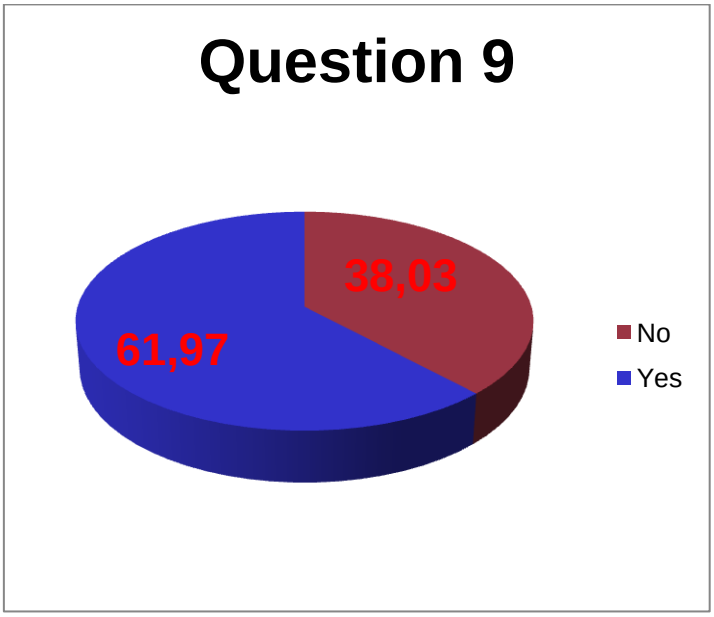

Figure 24: Result of Question 9 in Students Questionnaire

10. Which of the proposed methods would you prefer regarding trustfulness?

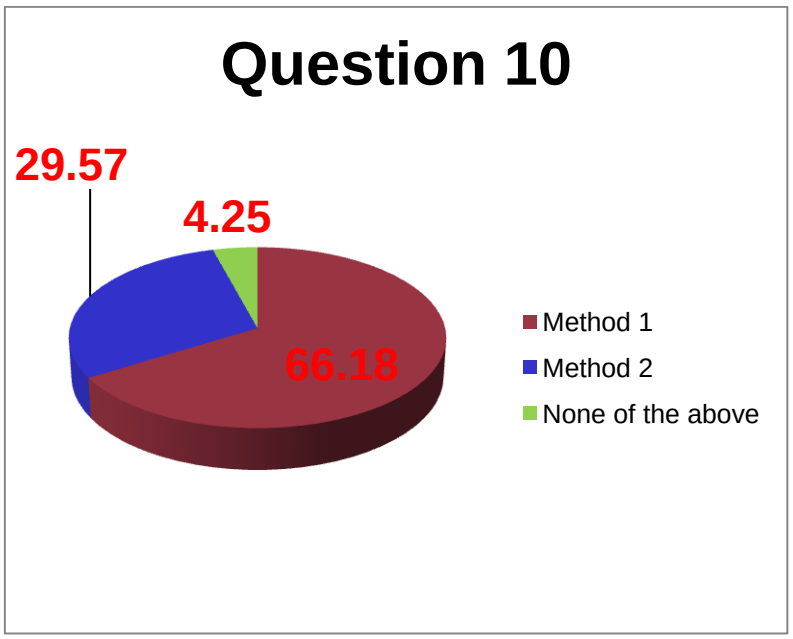

Figure 25: Result of Question 10 in Students Questionnaire

11. Which of the proposed methods would you prefer regarding ease of use?

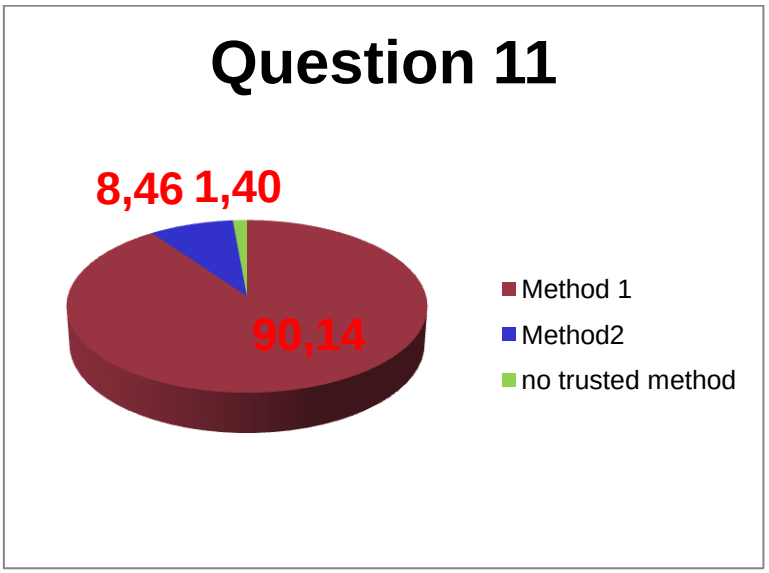

Figure 26: Result of Question 11 in Students Questionnaire

12. Which of the proposed methods would you prefer regarding efficiency?

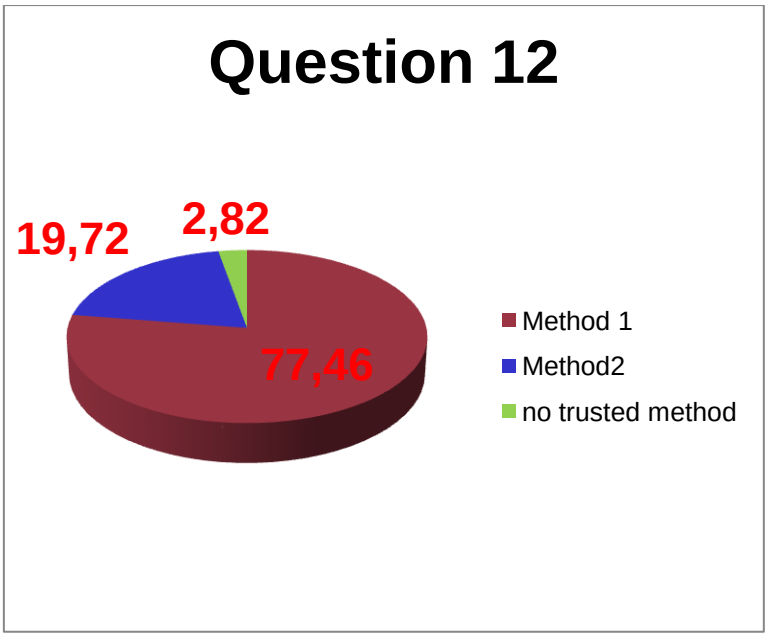

Figure 27: Result of Question 12 in Students Questionnaire

13. Regarding the First Method do you prefer to receive a 'proof' (e.g. a beep) that the transfer of the attendance information to your smart card was successful?

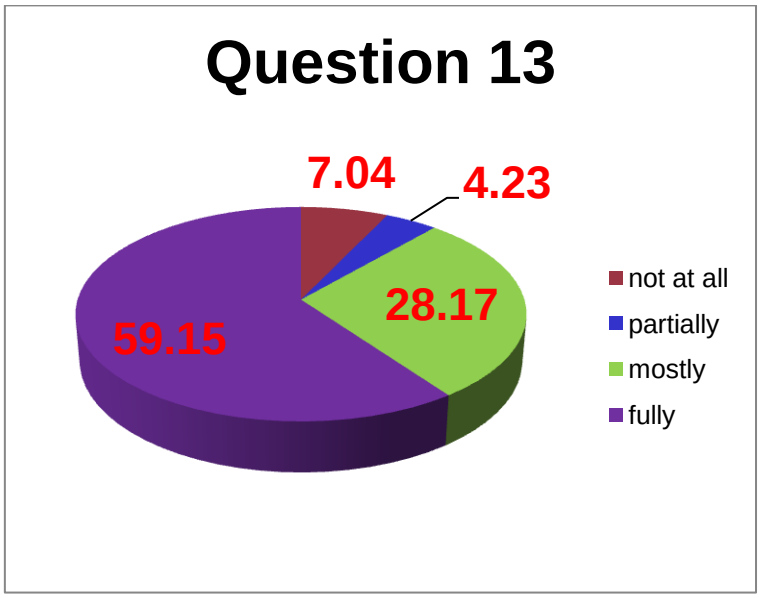

Figure 28: Result of Question 13 in Students Questionnaire

14. Regarding the Second Method do you believe that these codes will be forwarded by the professors to non-present students in order to get a higher percentage of course attendance in the statistics?

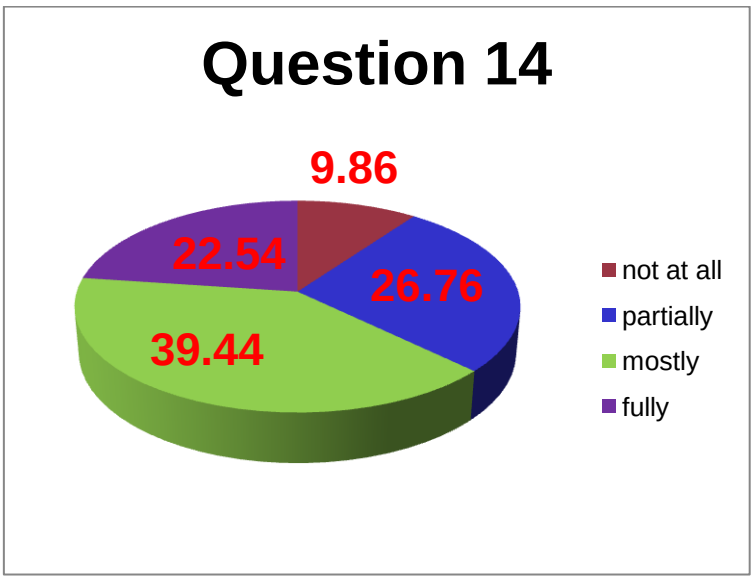

Figure 29: Result of Question 14 in Students Questionnaire

15. Please rate the importance of the following course poll goals.

1) Providing feedback to the lecturer so that the quality of the course is improved

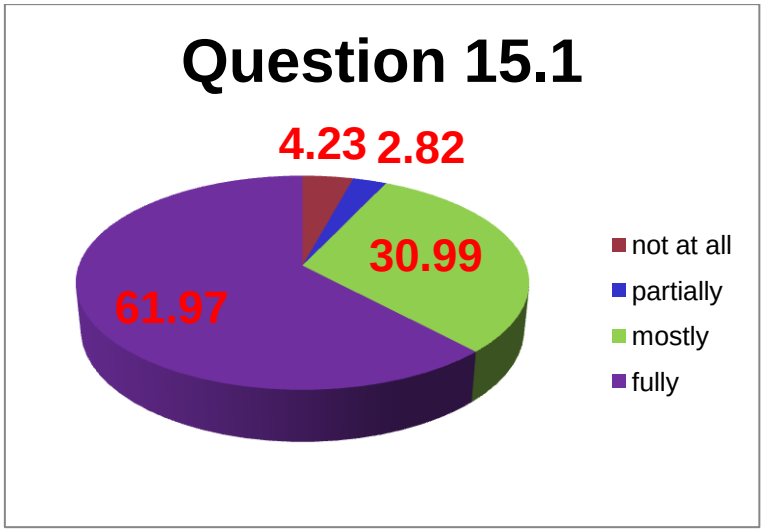

Figure 30: Result of Question 15.1 in Students Questionnaire

2) Evaluating the qualities of the professor

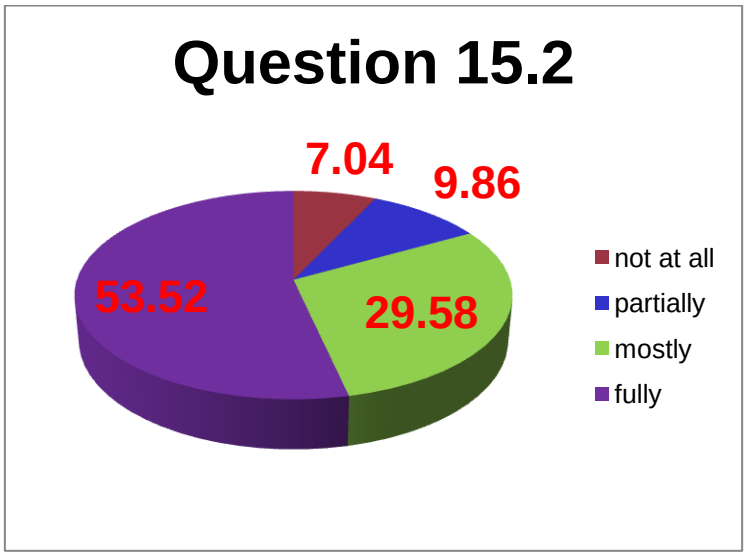

Figure 31: Result of Question 15.2 in Students Questionnaire

3) Refining the curriculum (e.g. delete unattractive courses)

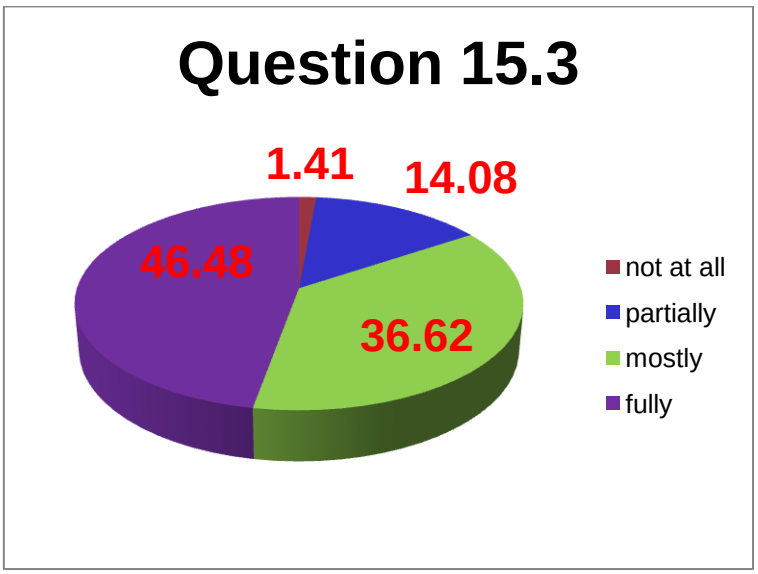

Figure 32: Result of Question 15.3 in Students Questionnaire

Students' Suggestions on question 15

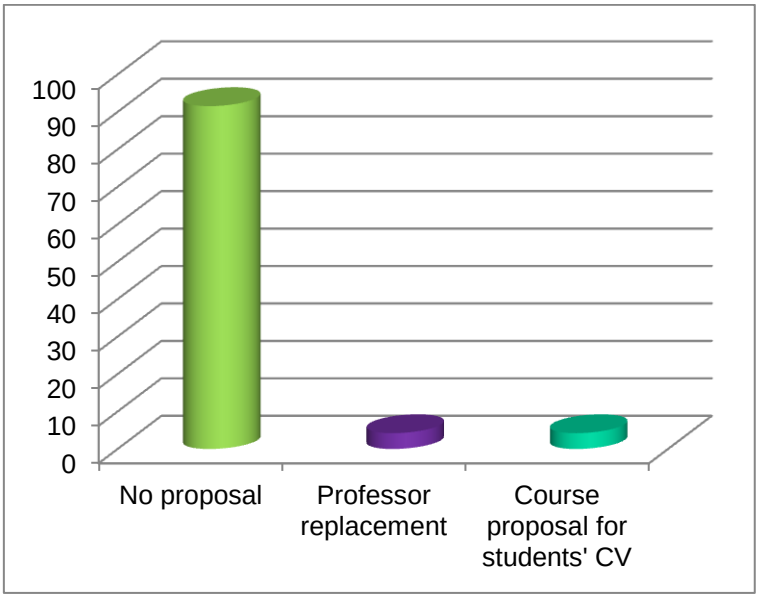

Figure 33: Students' Suggestion on Question 15 in Students Questionnaire

16)

1)Who should be able to read the results of a course evaluation?

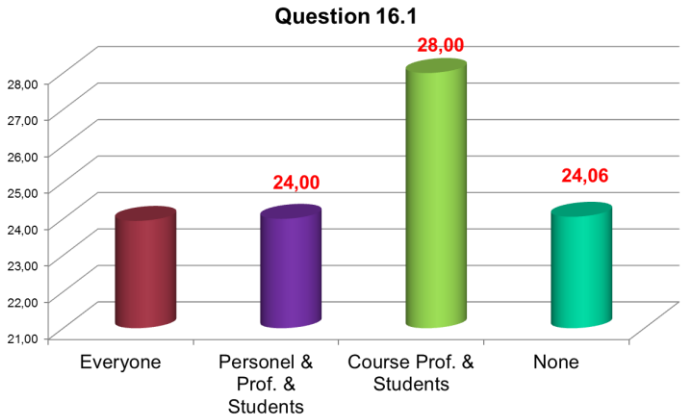

Figure 34:Result of Question 16.1 in Students Questionnaire

2) Students' Suggestions on Question 16

- professor council
- discussions of the results by students and the course professor
- only the course professor

A.2 Professor Questionnaire

A.2.1 Questionnaire Format

ABC4Trust Acceptance Questionnaire for Professors / Lecturers

Questions	Yes	No
2. Do you trust more an electronic evaluation system than a group of authorized people to perform the evaluation of a course?		
3. Can a reliable and trusted evaluation system collect data that can be used to improve the future courses?		
4. Do you expect the results of a course evaluation to be more reliable since the students' poll anonymously?		
5. Do you believe that using previous methods of course evaluation students hesitate to answer truthfully?		
6. Would you prefer a course evaluation system where the course questionnaire is adapted according to the course subject/material?		
7. Would you prefer a course evaluation system where different questions are presented to students according to their course attendance?		
8. Would you prefer a course evaluation system where different questions are presented to students according to their course performance?		
9. Would you prefer a course evaluation system where different weight is given to the opinion of the students according to their course attendance?		
10. Would you prefer a course evaluation system where different weight is given to the opinion of the students according to their course performance?		

Rate Table:

Score	1	2	3	4
	not important	somewhat important	important	extremely important

11. Please rate the importance of the following course poll goals, according to the above rate table. If you have any other suggestion, please write it.	
➢ Providing feedback to the lecturer so that the quality of the course is improved	
➢ Evaluating the qualities of the professor	
➢ Refining the curriculum (e.g. delete unattractive courses) ➢ Your suggestion:	

Please check only one answer to the following questions according your opinion. If you have any other suggestion, please write it.

12. Who should be able to read the results of a course evaluation?	
➢ Everyone (public results)	
➢ Personnel of the University including all students and all professors	
➢ Only students who attend the course and the corresponding professor ➢ Your suggestion:	

Question	Yes	No
13. Could the concept of digital credentials be applied to other aspects of your life?		

A.2.2 Results

1. Do you trust more an electronic evaluation system than a group of authorized people to perform the evaluation of a course?

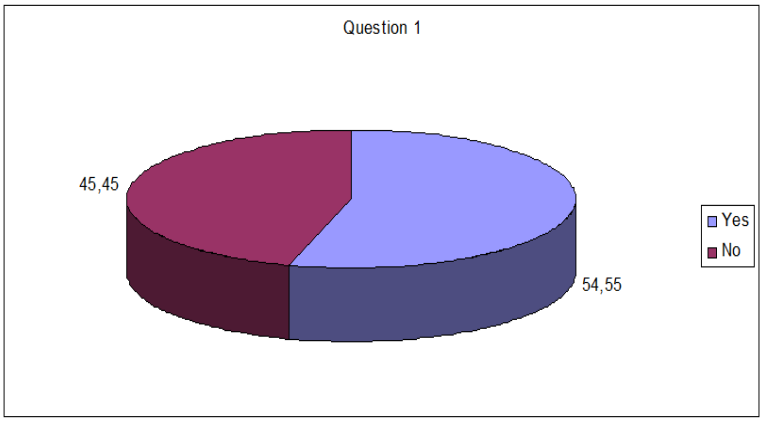

Figure 35: Result of Question 1 in Professors Questionnaire

2. Can a reliable and trusted evaluation system collect data that can be used to improve the future courses?

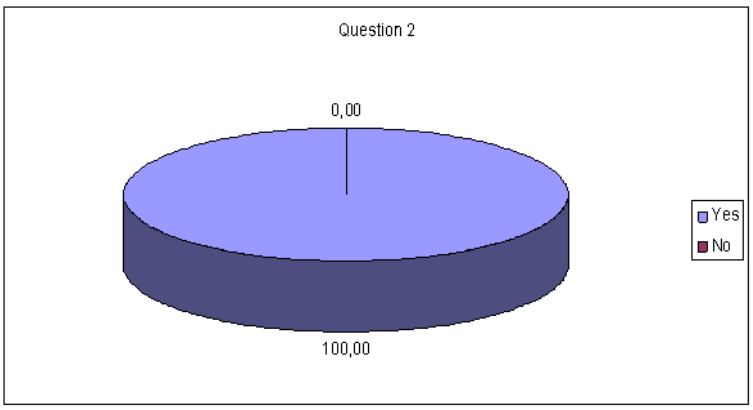

Figure 36: Result of Question 2 in Professors Questionnaire

3. Do you expect the results of a course evaluation to be more reliable since the students' poll anonymously?

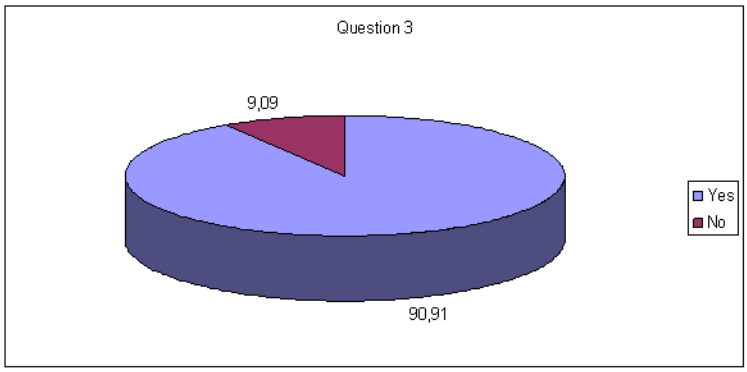

Figure 37: Result of Question 3 in Professors Questionnaire

4. Do you believe that using previous methods of course evaluation students hesitate to answer truthfully?

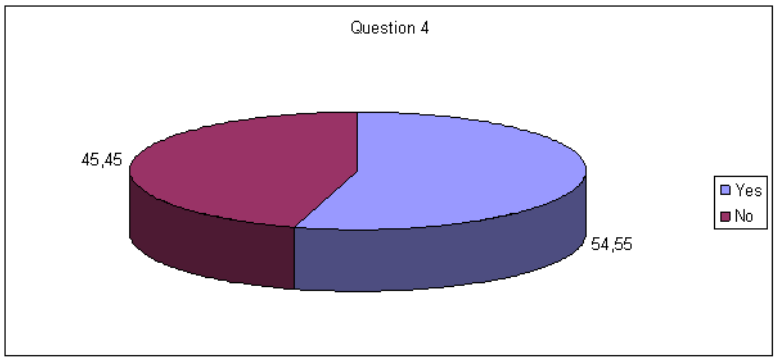

Figure 38:Result of Question 4 in Professors Questionnaire

5. Would you prefer a course evaluation system where the course questionnaire is adapted according to the course subject/material?
6.

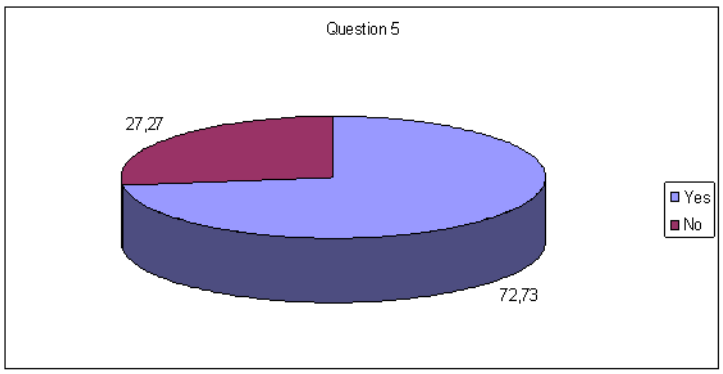

Figure 39: Result of Question 5 in Professors Questionnaire

7. Would you prefer a course evaluation system where different questions are presented to students according to their course attendance?

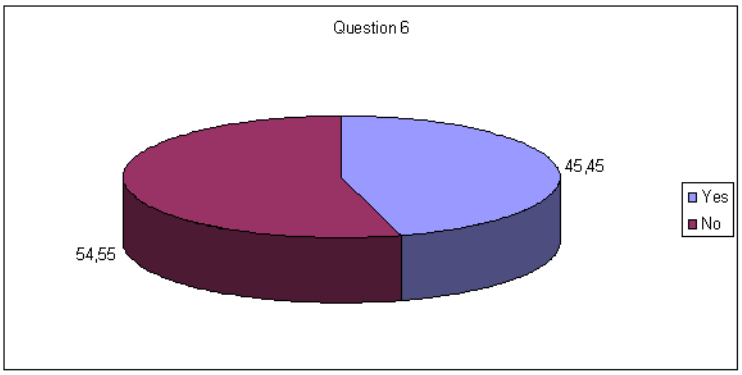

Figure 40: Result of Question 6 in Professors Questionnaire

8. Would you prefer a course evaluation system where different questions are presented to students according to their course performance?

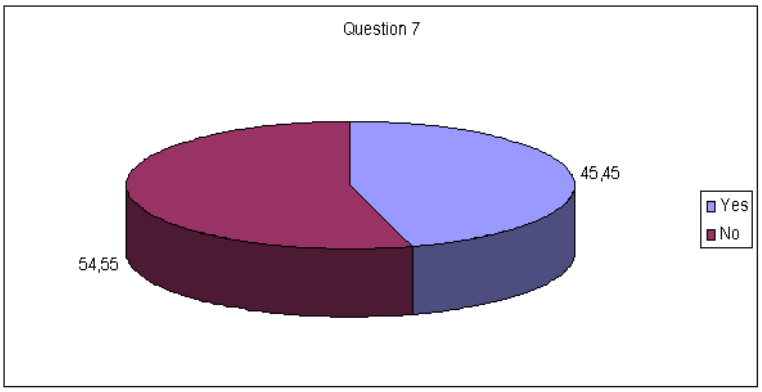

Figure 41: Result of Question 7 in Professors Questionnaire

9. Would you prefer a course evaluation system where different weight is given to the opinion of the students according to their course attendance?

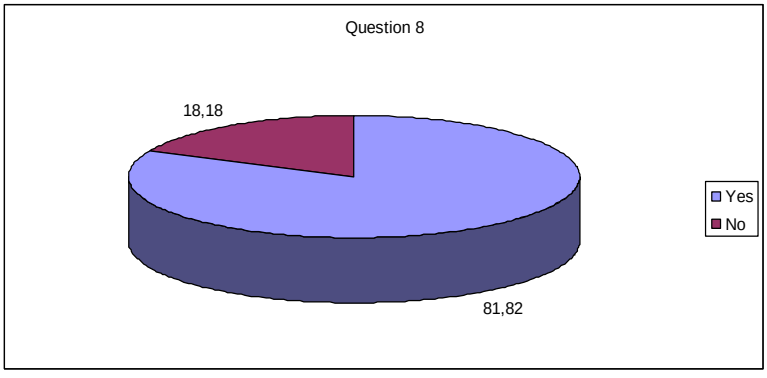

Figure 42: Result of Question 8 in Professors Questionnaire

10. Would you prefer a course evaluation system where different weight is given to the opinion of the students according to their course performance?

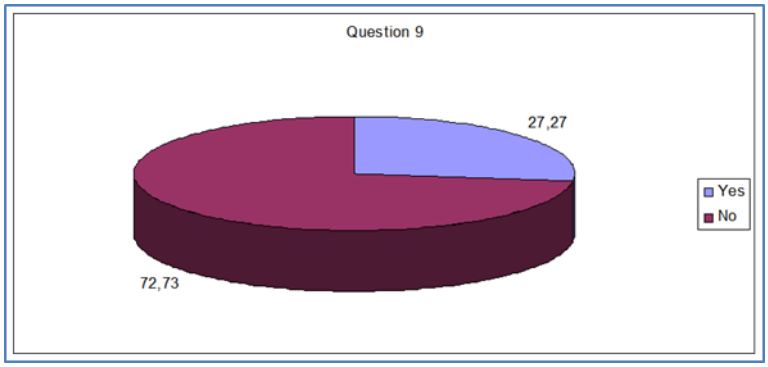

Figure 43: : Result of Question 9 in Professors Questionnaire

11. Please rate the importance of the following course poll goals.
    1) Providing feedback to the lecturer so that the quality of the course is improved

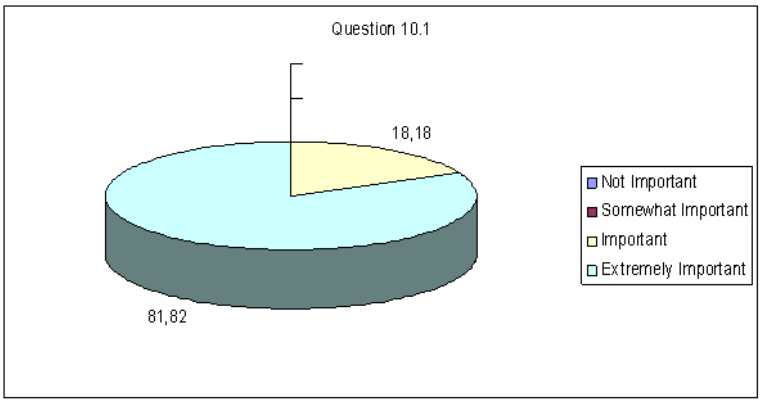

Figure 44: Result of Question 10.1 in Professors Questionnaire

    2) Evaluating the qualities of the professor

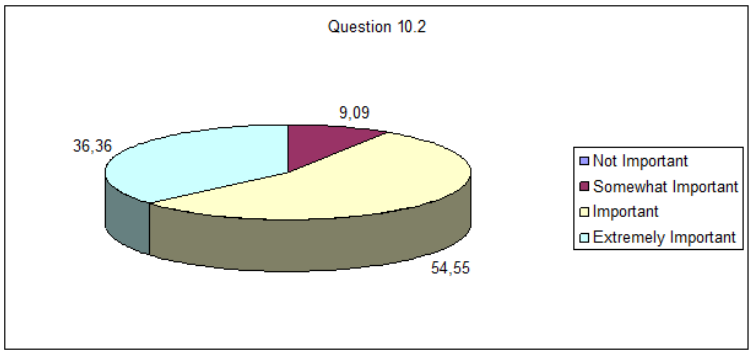

Figure 45: Result of Question 10.2 in Professors Questionnaire

3) Refining the curriculum (e.g. delete unattractive courses)

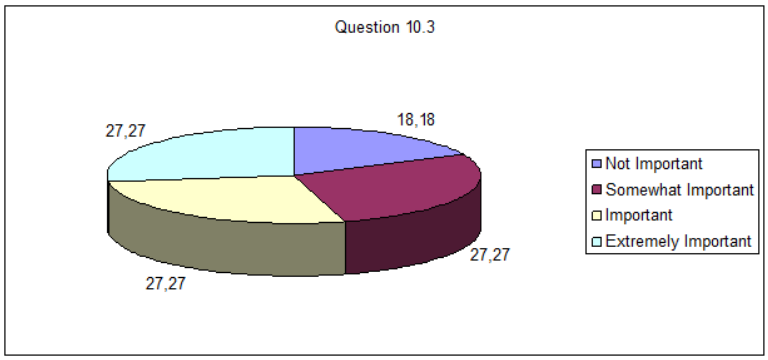

Figure 46: Result of Question 10.3 in Professors Questionnaire

12. Who should be able to read the results of a course evaluation?
    b) Everyone (public results)
    c) Personnel of the University including all students and all professors
    d) Only students who attend the course and the corresponding professor

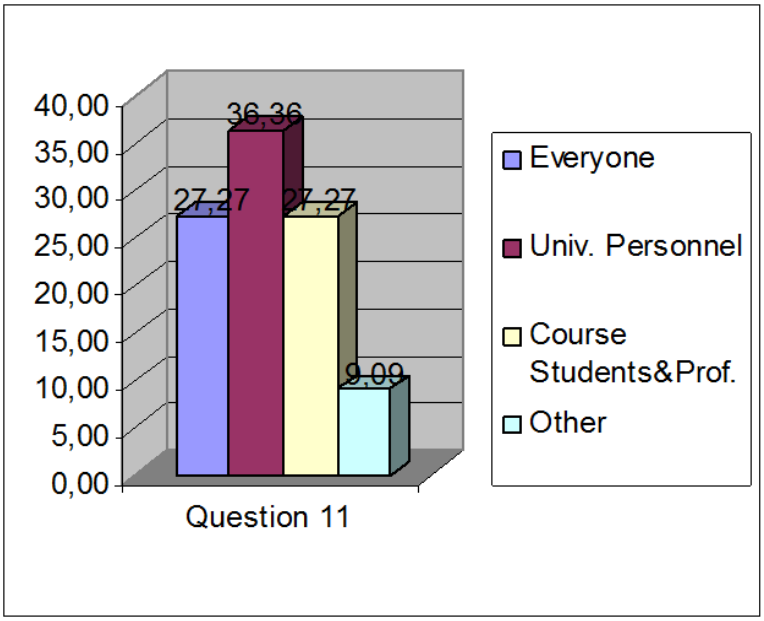

Figure 47: Result of Question 11 in Professors Questionnaire

12. Could the concept of digital credentials be applied to other aspects of your life?

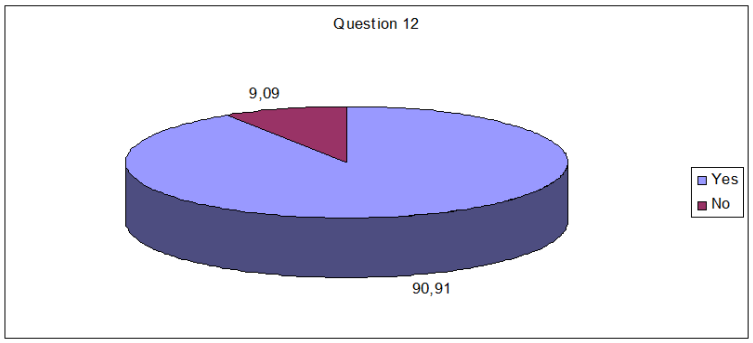

Figure 48: Result of Question 12 in Professors Questionnaire

Appendix B Conceptual Information Model of the University Pilot

Course Evaluation System is equipped with a database repository. This repository contains:

a. Evaluation Questionnaires

b. Course Information

c. User Pseudonyms

d. Evaluation Results

Regarding a:

The professor of a course is authorized to upload the Evaluation Questionnaire of his lesson (this could be implemented either by a simple access control system or by using ABC Technology). The professor can edit and modify the uploaded questionnaire several times until he finalizes it. The finalized questionnaire cannot be modified from anybody. The administrator has the authority to restart the upload procedure under the professor's request. The finalization of the questionnaire is a prerequisite for the activation of the course evaluation process.

Regarding b:

The course information includes a basic and general description of the course (e.g Course Name, Course Professor, etc.). Only the professor of the course can update this course information. When a professor successfully logs in, he can proceed with updating the course information.

Regarding c:

When a student accesses the Course Evaluation System in order to evaluate a course, he first interacts with the ABC System, which checks his ABC Credentials. If the check is successful, the ABC System forwards the student to the course evaluation application.

Regarding d:

When a student answers a questionnaire and submits, the Course Evaluation System stores his evaluation. The Course Evaluation System permits a student to evaluate a course multiple times. However, every new submission of an evaluation from the same student, replaces the previous one from that student.

Appendix C User manual

C.1 Introduction

Recently, much research has been done towards developing a number of technologies for building ABC systems in a way that they can be trusted, like well-known cryptographic PKI certificates, while at the same time protecting the privacy of their holder (e.g., hiding the real holder's identity). Such attribute-based credentials (Privacy-ABCs) are issued just like ordinary cryptographic credentials using a digital (secret) signature key. However, Privacy-ABCs allow their holder to transform them into a new token, in such a way that the privacy of the user is protected. Still, these transformed tokens can be verified just like ordinary cryptographic credentials and offer the same strong security.

The aim of ABC4Trust is to deepen the understanding in ABC technologies, enable their efficient/effective deployment in practice, and their federation in different domains. Towards this end, the ABC4Trust project aims to run the first ever pilots of ABC deployments in production environments. Thus, this will be the first time real user feedback on ABC systems will be collected. ABC4Trust will gather practical experience with ABC applications through two pilots which will be deployed in two specific environments: a school in Sweden and a University in Greece. This will give the opportunity to test Privacy-ABC's use and performance with two user groups of differing skills and needs. The pilots will provide feedback of distinct value to the developers of the reference implementation.

The University Pilot: The University Pilot is one of the two pilots that will take inside the ABC4Trust project. This pilot concerns the use of Privacy-ABCs for online course evaluation in the Computer Science department of the University of Patras, in Greece. CTI will be responsible for the deployment of the University pilot.

In this appendix we provide a brief introduction to the concepts of ABC4Trust and we explain the procedure for using the University Pilot system.

C.2 Basic concepts of ABC4Trust

C.2.1 Attribute-based Credentials

A *credential* is a certified container of attributes issued by an Issuer to a User (i.e. an entity possibly collecting credentials from various Issuers and controlling which information from which credentials she presents to which verifiers). An attribute is described by the *attribute type*, determining the semantics of the attribute (e.g., first name), and the *attribute value*, determining its contents (e.g., John). By issuing a credential, the Issuer vouches for the correctness of the contained attributes with respect to the User.

The User can then later use her credentials to provide certified information to a Verifier (for authentication or an access decision), by deriving *presentation tokens* that reveal partial information (in fact the minimum required information needed for the transaction) about the encoded attributes. Apart from revealing information about credential attributes, the presentation token can optionally sign an application-specific message and/or a random nonce to guarantee freshness. Moreover, presentation tokens support a number of advanced features such as pseudonyms, device binding, inspection, and revocation.

Presentation tokens based on Privacy-ABCs are in principle cryptographically unlinkable (although naturally, they are only as unlinkable as the information they intentionally reveal) and untraceable, meaning that Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials and that Issuers cannot trace a presentation token back to the issuance of the

underlying credentials. However, pseudonyms and inspection can be used to purposely create linkability across presentation tokens (e.g., to maintain state across sessions by the same User) and create traceability of presentation tokens (e.g., for accountability reasons in case of abuse).

There are a handful of proposals of how to realize an ABC system in the literature [Cha85, Bra93, CL01, CL04]. Notable is especially the appearance of two technologies, IBM's Identity Mixer and Microsoft's U-Prove, as well as extended work done in past EU projects. In particular, the EU-funded projects PRIME and PrimeLife have actually shown that the state-of-the art research prototypes of ABC systems can indeed confront the privacy challenges of identity management systems.

The PRIME project has designed an architecture for privacy-enhancing identity management that combines anonymous credentials with attribute-based access control, and anonymous communication. That project has further demonstrated the practical feasibility with a prototypical implementation of that architecture and demonstrators for application areas such as e-learning and location-based services. PRIME has, however, also uncovered that in order for these concepts to be applicable in practice further research is needed in the areas of user interfaces, policy languages, and infrastructures.

The PrimeLife project has set out in 2008 to take up these challenges and made successful steps towards solutions in these areas. For instance, it has shown that ABC systems can be employed on Smart Cards and thus address the requirements of privacy-protecting eID cards [BCGS09]. Also, in the last decade, a large number of research papers have been published solve probably all roadblocks to employ ABC technologies in practice. This includes means to revoke certificate [Ngu05, BDDD07, CL02, CKS09], protection of credentials from malware [Cam06], protection against credential abuse [CHK+06, CHL06], proving properties about certified attributes [CG08, CCS08], and means to revoke anonymity in case of misuse [CS03].

Despite all of this, the effort of understanding ABC technologies so-far was rather theoretical and limited to individual research prototypes. Indeed, so far, PRIME and PrimeLife only showed that ABC technologies provide privacy-protection in principle.

Furthermore, there are no commonly agreed set of functions, features, formats, protocols, and metrics to gauge and compare these ABC technologies, and it is hard to judge the pros and cons of the different technologies to understand which ones are best suited to which scenarios.

Thus, there is still a gap between the technical cryptography and protocol sides of these technologies and the reality of deploying them in production environments. A related problem with these emerging technologies is the lack of standards to deploy them. As a result the ENISA paper mentioned above observes that ABC "technologies have been available for a long time, but there has not been much adoption in mainstream applications and eID card applications" even though countries such as Austria and Germany have taken some important steps in this sense.

C.2.2 The ABC4Trust Project

The aim of ABC4Trust is to deepen the understanding in ABC technologies, enable their efficient/effective deployment in practice, and their federation in different domains. To this end, the project:

1. Produces an architectural framework for ABC technologies that allows different realizations of these technologies to coexist, be interchanged, and federated

    a. Identify and describe the different functional components of ABC technologies, e.g. for request and issue of credentials and for claims proof;

    b. Produce a specification of data formats, interfaces, and protocols formats for this framework;

2. Defines criteria to compare the properties of realizations of these components in different technologies; and

3. Provides reference implementations of each of these components.

With a comparative understanding of today's available ABC technologies, it will be easier for different user communities to decide which technology best serves them in which application scenario. It will also be easier to migrate to newer ABC technologies that will undoubtedly appear over time. In addition the same users may want to access applications requiring different ABC technologies, and the same applications may want to cater to user communities preferring different ABC technologies.

Hence, it is also necessary that different ABC technologies be able to coexist or be interchanged across scenarios involving the same users and application platforms. It may also be sometimes desirable to convert ABCs from one technology into another so as to federate them across different domains, as is done today between different authentication domains using standards such as SAML, WS-Trust, Kerberos, OpenID, or OAuth. There are no commonly agreed sets of functions, features, formats, protocols, and metrics to gauge and compare ABC technologies, so it is hard to judge their respective pros and cons. There is also currently no established practice or standard to allow for the interchangeability and federation of ABC technologies.

A number of countries have already introduced or are about to introduce electronic identity cards (eID) and drivers licenses. Electronic ticketing and toll systems are also widely used all over the world. As such electronic devices become widespread for identification, authentication, and payment (which links them to people through credit card systems) in a broad range of scenarios, the users' privacy and traceability will be increasingly threatened in the future internet society. If and when eIDs are rolled out, society and countries are well advised to build privacy protection techniques into them.

C.3 University Pilot Overview

The University Pilot will realize an evaluation where university students can anonymously evaluate courses they took while ensuring that students 1) have indeed taken the course and have attended sufficient number of lectures (i.e. attribute based credentials will be employed to prove these facts) and 2) can only rate the course once, without keeping list of students who have already rated the courses, so that the anonymity of the students is preserved.

In the University Pilot a group of students will take part in the evaluation of two courses they have attended at the University Department. The students have been informed of this evaluation at the beginning of the project and are kept in touch with the developments that correspond to the pilot's scenarios. There will be two rounds of course evaluation and an on-site testing of Course Evaluation by certified students so as to have as much feedback as possible to the reference architecture and implementation of the anonymous credentials platform. Moreover, preliminary questionnaires have been distributed to students and professors in order to collect and analyse their opinion with regard to several usage criteria of the anonymous credentials concept as well as the reference implementation. We plan to distribute complementary questionnaires in different phases of the Pilot deployment.

In the deployment of the University Pilot two essentially different credential technologies (namely the U-prove of Microsoft and the Idemix of IBM) will be integrated in a single platform. The purpose of the University Pilot is to experiment with all the aspects of these technologies, provide feedback for improvements and offer an overall assessment of their applicability, usability and effectiveness. In the following sections we describe environment and the users of the Pilot.

C.3.1 Objective(s) of the Patras Pilot

In University pilot university students can anonymously rate courses they took while ensuring that 1) students have indeed taken the course and have had sufficient attendance (i.e. attribute based credentials will be employed to prove these facts) and 2) can only rate the course once, without keeping list of students who have already rated the courses, so as to protect student anonymity.

More specifically, the objectives for the University pilot are:

1. Schedule and conduct research on a Course Evaluation system by certified students.
2. Define usage criteria for the Student Evaluation scenario.
3. Provide feedback to reference architecture and implementation.
4. Provide evaluation results useful to Users, Identity Service Providers, Relying Parties, and Standardization Bodies etc.

The major challenge is to ensure anonymous participation in a course evaluation which enables multiple evaluations (the last one will only be counted) and ensures unlinkability and confidentiality. In particular, only registered and eligible (e.g. to have attended over 2/3 of the course classes) students participate while not forcing them to provide details which may reveal identifying personal information. This can be achieved using Privacy-ABCs which will be defined in the University pilot. In particular, for each student a set of credentials will be defined in the context of the project that allows proving their eligibility for participating in a specific course evaluation. The students that will participate in the evaluation have 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.

The student credentials will be stored in smart cards and will be used to generate presentation tokens which are transmitted to the relying party's information system over the Internet (this scenario presupposes that the students use a smart card reader at the computer they use to provide their evaluations).

CTI will conduct two rounds of evaluation and an on-site testing of Course Evaluation by certified students. The students that will participate in the evaluation will be briefed on the scope and the goal of the pilot. Before the actual evaluations, CTI will select 3 to 5 student-volunteers in order to participate to an on-site testing of Course Evaluation by certified students. For the main course evaluations two groups of 25 students will take part in the evaluation of two courses (25 students for each course) that they have attended at a University Department. There will be two rounds of course evaluation: one in the first month of the fall semester of the year 2012 to evaluate a course whose examination will be performed in January 2013 and spring semester of the year 2013, to evaluate a course whose examination will be performed in June2013. This will assure that the second round of course evaluation will take advantage of the experience from the first as well as a new version of the reference implementation with corrections proposed during the first round of course evaluation. In order to assure that everything will operate as expected, CTI will conduct a small scale experimental on site course evaluation with 3-5 students equipped with smart cards in a mock up pilot setup. This will be when the reference implementation is ready by the end of April 2012.

C.3.2 Description of the pilot environment

The University Pilot will take place in the Computer Engineering and Informatics Department of the University of Patras in Greece. This is one of the most highly esteemed departments related to computer science in Greece. It is located very near to CTI premises. For the purposes of the University Pilot, a group of 30 students will take part in the evaluation of the following two courses:

- Operating Systems Laboratory: This is a compulsory course that takes place at the 6th semester and the number of students that attend it is approximately 200.
- Distributed Systems I: This is a non-compulsory course that takes place at the 7th semester and the number of students that attend it is approximately 60.

Course evaluations are a standard practice in Greek universities and are supported by the Hellenic Quality Assurance Agency for Higher Education (HQAA). The purpose of HQAA is to ensure the transparency of the evaluation procedure and also to guarantee that these procedures will be used in enhancing the quality of higher education.

However, up to date course evaluations in Greece are conducted on paper and they are done after class inside the lecture room. This unfortunately hinders the whole procedure, since the students need to put a lot of trust in the fairness and privacy practices of their university.

The University pilot realizes an electronic course evaluation in a way that ensures the credibility of results and preserves the privacy of the students expressing their opinion. More specifically, the system scope will be the realization of an evaluation where university students can anonymously rate courses they took while ensuring that: 1) participants are valid University of Patras students 2) participants are students that have indeed registered to the course and have had sufficient attendance and 3) participants can only rate the course once, without keeping list of students who have already rated the courses, so as to protect student anonymity.

C.3.3 User Community Description

The following table presents several properties for each User group present in the University Pilot.

User Group	Description / Expected Use of System	Geographic Location	Network Profile (LAN, WAN, External)	Total Users	Concurrent Users
Students	Certified Course Evaluation	University/Home	LAN, WAN	30	30
Professor	Upload Evaluation Questionnaire	University/Home	LAN, WAN	2	1
HQAA	Access Evaluation Results	University	LAN, WAN	1	1
Department Registration Employee	Import Students Data	University	LAN	1	1
Administrator	System Administration	CTI/NSN	LAN, WAN	3	1

Phd Students	NFC setup	CTI	LAN, WAN	2	2

C.3.4 University's Pilot Components

The Patras pilot is based on various components. These components have different functionalities and roles. Next, we describe the functionality and the characteristics of main components

Patras Portal: This component is an information web portal. Through this portal, the Users can be informed about the system's functionality and can be instructed on how to operate it. Thus, this page provides to the users the necessary links to the components of the system (e.g. University Registration System, Course Evaluation System) that are responsible for specific functionalities. Every time a user desires to interact with the system, her first action is to visit this portal and by following the instructions she can perform various pilot operations (e.g. register to a course, evaluate a course).

University Registration System: This component is mainly used for issuing Privacy-ABCs to the users of the system. Its sub-components are an ABC System, an IdM Application and the IdM portal. The IdM application is a web application whose potential users are students and university registration office employees. In particular:

- CTI with collaboration of a university registration office employee has the possibility to insert to the database of the University Registration System the personal information of the student-volunteers that will participate in the pilot. This activity does not require ABC technology.
- A university registration office employee can 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).
- Students can collect credentials that certify that they are valid students of the University of Patras
- Students are able to browse their personal data that is stored in the IdM database
- Students are able to administrate some of their personal data (e.g. course)
- Students can collect credentials that certify that they have registered to a course

When the IdM application is required to issue Privacy-ABCs to users (e.g. university credentials, course credentials) it invokes the ABC System which is responsible for performing the issuing protocols. When a user wants to browse her personal information, the IdM application uses the IdM portal that supports this functionality.

As the University Registration System is the main issuer of the Patras pilot, its parameters (system parameters, revocation information) should be stored in a public repository, so that all system components can access them. This repository is the IdM Public Directory that can be seen on the "High Level Architecture of the Patras pilot" figure.

Course Evaluation System: This component is responsible for the realization of the anonymous course evaluation process. Its sub-components are an ABC System and a Course Evaluation Application.

The ABC System is a component that performs access control to the Course Evaluation Application. This access control is achieved by presenting a policy to the potential users. Only users, who own credentials (e.g. course credential) that can be used to satisfy the access policy, are able to access the Course Evaluation Application.

The Course Evaluation Application is a web application that implements the functionality of the course evaluation procedure. Potential users of this application are students, professors and Hellenic

Quality Assurance Agency (HQAA) members. Hellenic Quality Assurance Agency is the legal authority that supervises any evaluation procedure in Greek Universities. In particular:

- Course professors have the possibility to upload questionnaires regarding their course and determine the threshold number of attended lectures required for participating in the evaluation. This activity does not require ABC technology.
- Students are able to evaluate courses that they have registered to and attended
- When the evaluation procedure is completed, CTI members will collect and process the evaluation results in order to provide accumulated course evaluation results to HQAA. This off-line activity does not require ABC technology.

Class Attendance System: This component is responsible for storing attendance data on the students' smart cards during the lecture of a course. It consists of an ABC System and a Class Attendance Application.

The equipment that is required for this component is a laptop and an NFC reader that is able to communicate through wireless communication with the students' smart cards. The Class Attendance Application runs on the laptop and is responsible for transferring (through the NFC reader) to the students' smart cards the attendance data related to specific course lectures. The ABC System will be used to issue attendance credentials to students with respect to their matriculation number.

User's Home Application: This component refers to the software that needs to be installed on the user's PC. Its main sub-component is an ABC System. The equipment that is required for this component is a smart card reader.

The ABC System provides to the user an interface between the browser and her smart card. For this reason, it employs a software component called "User Agent" that runs locally on her PC. This software component is triggered every time a user is required to provide data stored on her card and asks for her consent. Moreover, it enables the users to browse the Privacy-ABCs stored on their smart card, delete Privacy-ABCs and locally backup Privacy-ABCs.

C.4 Description of the Patras pilot

We have in mind the following basic phases that provide step-by-step descriptions of how the proposed system should operate and interact with its users under a given set of circumstances:

- The first phase concerns the initialization. After this phase all the systems are initiated and the students of Computer Engineering and Informatics Department have in their possession a smart card with a user secret.
- The second phase concerns the procedures required so that the students can obtain credentials that certify a number of facts about them.
- At the third phase, the students collect their attendance information. We also consider a phase which concerns that backing up and restoring students' attendance information, in order to handle smart card loss and retrieve the attendance data stored in students' smart cards, we define the phase that backups and restores students' attendance information.
- The last phase considers the course evaluation within the University of Patras.

C.4.1 Smart Cards Distribution

The student obtains her smart card and her smart card reader. In particular, the University Registration office distributes a sealed envelope, a smart card and a slip of paper containing a one-time-password (OTP) to each student that participates to the University pilot. The sealed envelope is marked with the

smart card ID and contains a PIN and a PUK. The slip of paper associates the envelope's identification number i.e. the smart card ID (provided to student) and the one-time-password. The smart card does not contain any personal information at that point. The University Registration office maintains a list of the correspondence between student names, envelope identification numbers (=smart card IDs) with corresponding OTPs.

C.4.2 User Secret Generation

The administrators of the Course Evaluation System, the University Registration System and the Class Attendance System initiate the operation of the corresponding systems for the first time (bootstrapping of the system). In particular, CTI with the collaboration of the University Registration office, provides the IDM database with the list of the correspondence between student names and envelope identification numbers (distributed to each student) and with the following certified attributes collected from the volunteering students that participate to the University pilot: (a) first name and last name, (b) University Name, (c) Department Name, (d) Matriculation Number.

At this point, each system administrator does the following:

- He generates the issuer parameters and the issuance keys for the issuers she is responsible for. In particular, this is done for the University Registration System and the Class Attendance System.
- The issuer parameters of the University Registration System are stored on the IdM public Directory and can be accessed by the ABC systems.

At some point after the parameters and the issuance keys are generated, each student participating in the University pilot can do the following (assuming the appropriate ABC software is installed on student's PC): She puts her smart card in the card reader and starts the initialization of the smart card, which requests her smart card PIN. In particular, the user secret will be generated which will be locked into the smart card. Also, the smart card will store the certificates of all trusted communication partners, as well as the issuer parameters of all authorized issuers in a tamper-proof area.

C.4.3 Obtaining the University/Course Registration Credential

This phase is the electronic version of the real life scenario that any student has to follow in order to be registered at University or pick a course. When a student wants to register at the University and obtain a valid student credential, she browses to the Patras portal and follows the provided instructions. University Registration system authenticates the student and initiates an issuance protocol that stores a valid student Privacy-ABC on her smart card. The student credential contains attributes related with personal student information (e.g. first name, last name, matriculation number)

A student wants to book a course and obtain a valid course credential. For this reason she browses to the Patras portal and follows the instructions in order to book the course. Student will get a valid course credential in her smart card by logging in University Registration system via ABC technology. The course credential stored in her smartcard contains attributes related with course information (e.g. course identifier).

C.4.4 Obtaining Class Attendance Data

All the students that will take part in the evaluation of two courses have to prove their attendance for a sufficient number of lectures without, however, revealing the exact attendance ratio and which lectures she visited. This phase uses the Class Attendance system in order to collect students' attendance information. Since Set up phase has finished all the students that will take part in the evaluation of two courses have been issued Privacy-ABCs that certify students' information (first name, last name, etc.)

and information related with the course. Student can log on to IDM portal and can view and administrate some of her own data using these credentials.

Class Attendance System will be placed in lecture room 15 minutes before the lecture starts. The Professor is responsible for fixing the exact times when each lecture of the course is happening (location, date, start and finish time). CTI in cooperation with PhD students will be responsible for the Class Attendance System's operation and physical security. Each student has to wave her smart cart in front of a contactless NFC reader when leaving the lecturing room, in order to collect her attendance information. Student smart-card is updated every time she attends a class.

C.4.5 Backup and Restore of Class Attendance Data

This phase is used in order to handle the loss of a smart card containing student's attendance information. Here, a student can back up her attendance information and to restore backed up data on her (new) smartcard.

We assume that the student attended some course lectures and has some attendance information stored on her smartcard. Student could run locally User Agent application on her PC in order to browse the Privacy-ABCs stored on her smart card, delete credentials or backup the smart card content on her PC. Student should connect her smart card reader to her PC before starting user agent application. The backup data must be encrypted by using user agent application for backing up.

If a student loses her smartcard then she can declare it lost to the University Registration Office where she can get a new envelope and smart card. If a student has backup smart card content on her PC, she will be able to restore backed up data from her PC on her (new) SC though User Agent application. In order to restore the attendance data, the User Agent application prompts student to enter her PIN. Note that the PIN for backup and restore can be selected by the user, thus may be different from the PIN for unlocking the SC. Student should connect her smart card reader to her PC before starting user agent application.

C.4.6 Revoking a Student's Privacy-ABCs

In some cases the University registration office has to be able to revoke a student's credential. As a first example, when a student has lost her smart card, she must declare her smart card lost to the University Registration Office where she can get a new envelope (containing PIN, PUK) and a smart card. The University Registration System Administrator revokes the student University credential and deletes the student's private information from the ABC system. Then the student has to obtain a valid student and course credential and she will be able to use the backup data from her PC.

As a second example, when a student graduates and she is no longer a valid student the University registration office has to be able to revoke student's credential. The University Registration System Administrator revokes the student University credential and deletes the student's private information from the ABC system.

C.4.7 Course Evaluation

A group of students will take part in the evaluation of two courses they have attended at a University Department. We assume that the set up phase has been finished and all the students that will participate at the evaluation have at their possession a valid student credential and one or more course credentials. Then only students who can prove sufficient attendance of a specific course may participate in the evaluation process of this course. Thus the students should have stored sufficiently many attendance credentials in her SC.

This Course Evaluation is used for the realization of the course evaluation. Before the end of semester the HQAA will cooperate with the Department in order to distribute a general template of course

evaluation questionnaire to professors. The professor has to customize the course evaluation questionnaire to suit the course's needs. After this, the professor submits the course questionnaire using the course evaluation application. After the final exam has taken place, the students will be able to evaluate the course at any time from their home. Each student should have an ABC4Trust SC reader and have installed the ABC user agent on her computer in order to start the course evaluation procedure. Students are able to participate anonymously in a course evaluation by logging in to the Course Evaluation System via ABC technology. Whenever a student wants to evaluate a course she can access the Patras portal though her computer and the smart card reader. Then the Patras Portal will redirect him to the course evaluation system where only users satisfying certain policies will be able to access. If the Course Evaluation System is not online or if the Course Evaluation System is not yet enabled, the student will receive a suitable notification. The student will be able to fill in the uploaded questionnaire if she satisfies the following policies:

- The student is a valid Patras University student
- The student has indeed booked the course
- The student has had sufficient attendance credits through the semester

When a student satisfies these policies the Course Evaluation System prompts the student to fill in the evaluation form and stores the result of the last submitted course evaluation. If the student does not satisfy all the above three policies, she will receive a notification process and the evaluation process will be terminated.

Each student is allowed to evaluate multiple times but only the last evaluation is taken into account (to ensure that the student's evaluation was not a result of coercion). The Course Evaluation Application will consist of a database for storing policies and evaluation data. If the policies that specify the eligibility of students to answer a question lead to a small and possibly identifiable subset of students, then the system should prevent the students from answering the question. The HQAA will be invited to cooperate with the Department for the dissemination of the evaluation results.

C.5 Glossary

Anonymous

> Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set.

Attribute

> A piece of information, possibly certified by a credential, describing a characteristic of a natural person or entity, or of the credential itself. An attribute consists of an attribute type determining the semantics of the attribute (e.g., first name) and an attribute value determining its contents (e.g., John).

Certified pseudonym

> A verifiable pseudonym based on a user secret that also underlies an issued credential. A certified pseudonym is established in a presentation token that also demonstrates possession of a credential bound to the same User (i.e., to the same user secret) as the pseudonym.

Credential

> A list of certified attributes issued by an Issuer to a User. By issuing a credential, the Issuer vouches for the correctness of the contained attributes with respect to the User.

Credential specification

> A data artifact specifying the list of attribute types that are encoded in a credential.

Data Controller

> "'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data...", Art. 2 (d) of Directive 95/46/EC. In the area of Privacy-ABCs the Issuer, Verifier, the Revocation Authority and the Inspector are Data Controllers with the respective duties arising from the law.

Data Processor

> "'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller", Art. 2 (e) of Directive 95/46/EC. Data Controllers processes personal data on behalf of the data Controller.

Data Subject

> A data subject is an identified or identifiable natural person, Art. 2 (a) of Directive 95/46/EC. In the area of Privacy-ABCs the User and any other national person of which personal data is processes is a data subject. Data subjects have data subjects' rights assigned such as the right of access, rectification, erasure and blocking, Art. 12 of Directive 95/46/EC.

Device binding

> An optional credential feature whereby the credential is bound to a strong secret embedded in a dedicated hardware device so that any presentation token involving the credential requires the presence of the device.

Entity

> Entity is anything that has a distinct existence; it is the fundamental "thing" that can be identified.
>
> 1. Digital entity is any Entity which primarily exists in some digital context, e.g., as a digitally encoded information or as a running computer program.
> 2. Legal entity is any Entity which has some sort of legal subjectivity, or which is legally recognized in a judicial system. *For the commentary text: Examples include besides natural persons (humans) also companies that have been granted legal subjectivity by the law such as stock corporations, limited liability companies etc.*
> 3. Physical entity is an entity for which some sort of physical constituent is compulsory.

Inspection

> An optional feature allowing a presentation token to be de-anonymized by a dedicated Inspector. At the time of creating the presentation token, the User is aware (through the presentation policy) of the identity of the Inspector and the valid grounds for inspection.

Inspection grounds

> The circumstances under which a Verifier may ask an Inspector to trace the User who created a given presentation token.

Inspection Requester

> Entity requesting an inspection from the Inspector, asserting that inspection is compliant with the inspection grounds specified or is legally required. In most cases this will be the Verifier, but also may be the police, or other legally authorised entity.

Inspector

> A trusted entity that can trace the User who created a presentation token by revealing attributes from the presentation token that were originally hidden from the Verifier.

Issuance key

The Issuer's secret cryptographic key used to issue credentials.

Issuer

The party who vouches for the validity of one or more attributes of a User, by issuing a credential to the User.

Issuer parameters

A public data artifact containing cryptographic and other information by means of which presentation tokens derived from credentials issued by the Issuer can be verified.

Linkability

See *unlinkability*.

Personal data

"'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to her physical, physiological, mental, economic, cultural or social identity", Art. 2 (a) of Directive 95/46/EC. Within this deliverable personal data is the terminology used for legal considerations. See also *Personally Identifiable Information*.

Personally Identifiable Information (PII)

Personally Identifiable Information is defined as any information about an individual maintained by an [entity], including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, and any other information that is linked or linkable to an individual ([NIST10] p. 2-1). PII is a widely used terminology for *personal data* in the domain of information security. Within this document PII is used in relation to information security.

Presentation policy

A policy created and published by a Verifier specifying the class of presentation tokens that the Verifier will accept. The presentation policy contains, among other things, which credentials from which Issuers it accepts and which information a presentation token must reveal from these credentials.

Presentation token

A collection of information derived from a set of credentials, usually created and sent by a User to authenticate to a Verifier. A presentation token can contain information from several credentials, reveal attribute values, prove that attribute values satisfy predicates, sign an application-specific message or nonce or support advanced features such as pseudonyms, device binding, inspection, and revocation. The presentation token consists of the presentation token description, containing a technology-agnostic description of the revealed information, and the presentation token evidence, containing opaque technology-specific cryptographic parameters in support of the token.

Pseudonym

See *verifiable pseudonym*.

Pseudonym scope

A string provided in the Verifier's presentation policy as a hint to the User which previously established pseudonym she can use, or to which a new pseudonym should be associated. A

single User (with a single user secret) can generate multiple verifiable or certified pseudonyms for the same scope string, but can only generate a single scope-exclusive pseudonym.

Pseudonymous

The state where an Entity (User) is known to a party (Verifier, Issuer) by a Pseudonym, i.e., by a Partial Identity.

Revocation

The act of withdrawing the validity of a previously issued credential. Revocation is performed by a dedicated Revocation Authority, which could be the Issuer, the Verifier, or an independent third party. Which Revocation Authorities must be taken into account can be specified by the Issuer in the issuer parameters (Issuer-driven revocation) or by the Verifier in the presentation policy (Verifier-driven revocation).

Revocation Authority

The entity in charge of revoking credentials. The Revocation Authority can be an Issuer, a Relying Party, or an independent entity. Multiple Issuers or Verifiers may rely on the same Revocation Authority.

Revocation information

The public information that a Revocation Authority publishes every time a new credential is revoked or at regular time intervals to allow Verifiers to check that a presentation token was not derived from revoked credentials.

Revocation parameters

The public information related to a Revocation Authority, containing cryptographic information as well as instructions where and how the most recent revocation information and non-revocation evidence can be obtained. The revocation parameters are static, i.e., they do not change every time a new credential is revoked or at regular time intervals like the revocation information and non-revocation evidence (may) do.

Non-revocation evidence

The User-specific or credential-specific information that the user agent maintains, allowing it to prove in presentation tokens that the credential was not revoked. The non-revocation evidence may need to be updated either at regular time intervals or when new credentials are revoked.

Scope

See *pseudonym scope.*

Scope-exclusive pseudonym

A certified pseudonym that is guaranteed to be cryptographically unique per scope string and per user secret. Meaning, from a single user-bound credential, only a single scope-exclusive pseudonym can be generated for the same scope string.

Traceability

See *untraceability*.

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.

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.

User

The human entity who wants to access a resource controlled by a verifier and obtains credentials from Issuers to this end.

User agent

The software entity that represents the human User and manages her credentials.

User binding

An optional credential feature whereby the credential is bound to an underlying user secret. By requiring multiple credentials to be bound to the same user secret, one can prevent Users from "pooling" their credentials.

User secret

A piece of secret information known to a User (either a strong random secret or a human-memorizable password or PIN code) underlying one or more issued credentials or pseudonyms. A presentation token involving a pseudonym or a user-bound credential implicitly proves knowledge of the underlying user secret.

Verifiable pseudonym

A public identifier derived from a user secret allowing a User to voluntarily link different presentation tokens created by her or to re-authenticate under a previously established pseudonym by proving knowledge of the user secret. Multiple unlinkable pseudonyms can be derived from the same user secret.

Verifier

The party that protects access to a resource by verifying presentation tokens to check whether a User has the requested attributes. The Verifier only accepts credentials from Issuers that it trusts

C.6 Acronyms

ABCs

Attribute Based Credentials

Privacy-ABCs

Privacy Attribute Based Credentials (privacy-ABCs)

ABCE

ABC Engine

CA

Certificate Authority

CE

Crypto Engine

DFD

Data Flow Diagrams

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 Manager

ISP

Internet Service Provider

NFC

Near Field Communication

PC

Personal Computer

PIN

Personal Identification Number

PUK

PIN Unlock Key

RP

Relying Party

SC

Smart Card

SCI

Smart Card Interface

SSL

Secure Sockets Layer

STS

Secure Token Service

TTP

Trusted Third Party

TLS

Transport Layer Security

URI

Uniform Resource Identifier

WP

Work Package

XML

eXtensible Markup Language

C.7 Bibliography

[BCGS09] Patrik Bichsel, Jan Camenisch, Thomas Groß, and Victor Shoup. Anonymous credentials on a standard java card. In Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, pages 600–610, New York, NY, USA, 2009. ACM.

[BDDD07] Stefan Brands, Liesje Demuynck, and Bart De Decker. A practical system for globally revoking the unlinkable pseudonyms of unknown users. In Proceedings of the 12th Australasian Conference on Information Security and Privacy, ACISP'07, pages 400–415, Berlin, Heidelberg, 2007. Springer-Verlag.

[Bra93] Stefan Brands. Untraceable off-line cash in wallets with observers (extended abstract). In CRYPTO, pages 302–318, 1993.

[Cam06] Jan Camenisch. Protecting (anonymous) credentials with the trusted computing group's TPM v1.2. In SEC, pages 135–147, 2006.

[CCS08] Jan Camenisch, Rafik Chaabouni, and Abhi Shelat. Efficient protocols for set membership and range proofs. In ASIACRYPT, pages 234–252, 2008.

[CG08] Jan Camenisch and Thomas Groß. Efficient attributes for anonymous credentials. In ACM Conference on Computer and Communications Security, pages 345–356, 2008.

[CHK+06] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to win the clone wars: efficient periodic n-times anonymous authentication. In ACM Conference on Computer and Communications Security, pages 201–210, 2006.

[CHL06] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Balancing accountability and privacy using e-cash (extended abstract). In SCN, pages 141–155, 2006.

[CKS09] Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In Public Key Cryptography, pages 481–500, 2009.

[CL01] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In EUROCRYPT,

pages 93–118, 2001.

[CL02] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In CRYPTO, pages 61–76, 2002.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In CRYPTO, pages 56–72, 2004.

[CS03] Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In CRYPTO, pages 126–144, 2003.

[Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. Commun. ACM, Vol. 28, No. 10, pages 1030–1044, 1985.

[Ngu05] Lan Nguyen. Accumulators from bilinear pairings and applications. In CT-RSA, pages 275–292, 2005.