Privacy Preserving Course Evaluations in Greek Higher Education Institutes: An e-Participation Case Study with the Empowerment of Attribute Based Credentials

Vasiliki Liagkou[1], George Metakides[1], Apostolis Pyrgelis[1], Christoforos Raptopoulos[1], Paul Spirakis[1,2], and Yannis C. Stamatiou[1,2,3]

[1] Computer Technology Institute & Press – "Diophantus",
N. Kazantzaki Str., 26504 Patras, Greece
{liagkou,spirakis}@cti.gr, {pyrgelis,raptopox,stamatiu}@ceid.upatras.gr,
george@metakides.net

[2] Computer Engineering and Informatics Department,
University of Patras, 26504, Rio, Patras, Greece

[3] Business Administration Department,
University of Patras, 26504, Rio, Patras, Greece

Abstract. Course evaluations enable educational institutions to adjust their teaching methodologies and curricula in order to suit, best, their students' needs. Such evaluations in Greece are being conducted for many years in higher education institutes based on traditional print questionnaires handed-out to students at the lecture room. Compared to traditional paper-based questionnaires, the introduction of electronic student evaluation procedures has a number of advantages that merit consideration. a) it allows the students to evaluate courses from their home at their ease and beyond privacy breaches (e.g. by avoiding his/her fellow student looking at his/her answers), b) results are automatically archived in electronic format allowing fast further processing for the extraction of useful information, and c) it offers the possibility of using strong cryptographic tools to ensure student anonymity and data confidentiality. In this report we describe a pilot system that is being developed by the Computer Technology Institute & Press - "Diophantus" (CTI) within the context of the project ABC4Trust. The project's main goal is the development of a reference implementation of a privacy preserving eIdentity management framework based on the cryptographic primitives called Attribute Based Credentials. The pilot system will offer to a group of selected students the possibility of evaluating courses they have taken from their homes through the Internet and provide their feedback proving their eligibility to participate in the evaluation while, at the same time, preserving their anonymity. In this paper we describe the architecture and main scenarios of the pilot. CTI's long term vision is to use the pilot as a small scale proof of concept of privacy enhancement technologies in the eParticipation domain in order to introduce, in the future, of these technologies to the educational communities of all levels in Greece. These technologies will be the vehicle for supporting privacy preserving eParticipation in

B. Preneel and D. Ikonomou (Eds.): APF 2012, LNCS 8319, pp. 140–156, 2014.
© Springer-Verlag Berlin Heidelberg 2014

discussion groups whereby participants will provide their opinion anonymously but after proving that they are eligible to participate in group discussions.

1 Introduction

Over the last years the widespread use of the Internet and the new technologies by increasing volumes of population has made possible the creation of public consultation fora and opinion gathering platforms towards the realization of the concepts of eParticipation and eGovernance as integral parts of modern democracies. We have entered in a phase where old government-centric practices are strongly challenged and citizens demand direct involvement in social collective and political issues. One of the main obstacles for the wide adoption of eParticipation tools, such as polling and opinion gathering, is the reluctance of citizens to participate. This reluctance can be, partially, attributed to the, relatively, low penetration of technology among citizens (especially those of higher ages). However, the main reason behind this reluctance is the lack of trust towards ICT, which stems from the fear of citizens that systems implementing eParticipation services and procedures may violate their privacy. Our point of view, which we will discuss in the proposed chapter, is that trust in ICT-based Government should be founded on the emergence of the belief, on the citizens' side, that the systems implementing eParticipatiin respect their privacy. The departure point of our approach is that the emergence of such a belief can be considerably facilitated by designing and building systems in a way that demonstrates the respect in privacy using tools and representations that can be understood and checked by the specialist and, to a certain degree, by the layman alike. These tools and representations should provide sufficient evidence that the target system indeed handles privacy concerns and requirements to a degree that can, at least, eliminate the reluctance towards eParticipation. The ABC4Trust project, to the consortium of which CTI belongs, aims to deepen the understanding of a new privacy preserving, eIdentity management technology, based on Attribute Based Credentials. This technology enables the user to uncover only the elements of his/her eIdentity which are required in order to prove his/her eligibility in using a service. In addition, the project will organize and run the first ever pilots of ABC deployment in two real application environments, collecting useful feedback from the users that will participate in the pilots. One pilot will be performed in Sweden and will develop a privacy respecting public consultation and discussion environment for secondary school pupils while the other pilot will involve, in a privacy preserving manner, a number of University students to perform electronic evaluation of a course they have attended at the University. ABC4Trust will accumulate invaluable 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.

In this paper we will focus on the Greek pilot, which concerns remote course evaluation of university courses. The pilot scenario and set-up, which will be explained in detail in the rest of the paper, are as follows: The students will be issued credentials that certify a number of facts about them (e.g. year of study, major, number of times students appeared in lectures, etc.), allowing student with proper credentials to anonymously provide feedback on courses and instructors they had during a semester or school year. To be eligible to participate, the students' credentials should prove some facts about them, i.e. whether they have taken the course, the year of their first registration to the university department, and their the exact course attendance information (i.e. exact number of times the students actually appeared in lectures). All this should be done without revealing any elements that uniquely identify the student. This privacy 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, proof that they have attended sufficient number of classes, indication of grade level (e.g. pass/fail, without indication of exact grade) etc.). The student credentials are stored in their smart cards and are verified (without ever the credentials leaving the card) by the relying party for compliance with the relying party's access policy.

There will be two pilot rounds over the 2012-2013 academic year. The first round will be run within the fall 2012 semester and the other round will be run within the spring 2013 semester. This will assure that the second trial will take into advantage the experience from the first as well as a new version of the reference implementation with corrections proposed during the first trial. CTI's plans is to use this pilot as means of introducing ABCs first to the educational community of Greece as a tool for opinion gathering of certified group members and then to the Greek government as an eParticipation tool that respects users' privacy. Our belief is that innovations, such as ABCs, that can introduce breakthroughs in privacy respecting eIdentity management are more likely to be adopted and trusted by people if they are introduced gradually, in a step-wise manner, from specialized technical groups of people to more general non-technical groups and not in an "all-inclusive manner", which may be viewed by many as an abrupt, intrusive effort to interfere with people's everyday lives and ways of conduct.

2 The Core ABC Ideas and the ABC4Trust Project

2.1 Privacy and Privacy ABCs

Commonly used user authentication methods (e.g. PKI based) that are employed today for controlling access to Internet services most often fall short, with regard to respecting users' *privacy.* In general this situation arises in services in which only a *subset* of a user's full identity profile is necessary to allow access to a service. Such services range from accessing online libraries, where there is no need to give full identity profile to access books but only a proof that you are subscribed to the library, to online borrowing of movies, where you may have to prove that you are of appropriate age (e.g. older than 18) in order to watch particular films. In such types of applications there is, clearly, a need for a *partial*, and not complete, revelation of the user's identity.

Privacy Attribute-Based Credentials or Privacy-ABCs, for short, is a technology that enables privacy preserving, partial authentication of users. Privacy-ABCs are issued just like normal electronic credentials (e.g. PKI based) using a secret signature key owned by the credential issuer. However, and this is a key feature of this technology, the user is in position to transform the credentials into a new form, called *presentation token*, that reveals only the information about him which is really necessary in order to access a service. This new token can be verified with the issuer's public key.

The main ABC entities are four: the *Issuer*, the *User*, the *Verifier*, and the *Revocation Authority*. In general, the Issuer issues credentials containing certified user attributes, thereby attesting the validity of the attributes. The Verifier, or *relying party*, on the other hand, offers a service with access limited only to those users for which it can verify the possession of certain attributes (or credentials). The Revocation Authority is responsible for revoking issued credentials, i.e. disabling the possibility of creating presentation tokens out of them.

2.2 The ABC4Trust Project

Some proposals of how to realize ABC systems in the literature can be found in [3–5]. Notable in this respect has been the appearance of two technologies, *IBM's Identity Mixer* and *Microsoft's U-Prove*, as well as some preliminary work done in past EU projects. More precisely, 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 in today's Internet applications.

However, even though PRIME and PrimeLife showed that ABC technologies can provide, in principle, privacy respecting user authentication, the emphasis of understanding ABC technologies was rather on their theoretical analysis. Moreover, no agreed upon set of functionalities, information formats, and protocols has appeared in a prototype or set of libraries form that can boost the applicability and wide acceptance of ABC technologies further. Accordingly, a gap existed between the theoretical ABC proposals and the real user authentication applications. This gap was, further, magnified due to the lack of standardization in the ABC domain. As a result, the *European Network and Information Security Agency* (ENISA) observed in [2] that although ABC technologies have been available for a long time, no steps have been taken towards their adoption in mainstream user authentication and eIdentity card applications (however, countries such as Austria and Germany have taken some important steps towards this direction).

The ABC4Trust project (see [1]) aims at eliminating the gap between theory and practice in ABC technologies in order to pave the way towards their deployment in applications requiring partial user authentication. In particular, the project's two main goals are (i) to propose an architectural framework for Privacy-ABC technologies that allows their co-existence and interchangeability (e.g. IBM's Idemix and Microsoft's U-Prove) and (ii) to provide a reference implementation of those ABC components that developers can deploy in order to build privacy enhanced technologies in their own applications. A key element of the project in demonstrating the practical use of ABC technologies is the implementation of two ABC based pilot applications: one to be run in a school in Sweden and one to be run at a University in Greece. This paper focuses on the second pilot.

3 Towards Electronic University Course Evaluations

Course evaluations have become, today, a standard practice in most universities around the world. However, these evaluations are most frequently conducted by traditional means: students who happen to be in the lecture room on the day the evaluation is scheduled are handed paper-based questionnaires which they have to complete *anonymously* while the instructor waits outside. The anonymity and absence of the instructor requirements protect student's privacy. In cases where the evaluations are conducted electronically, the employed infrastructure does not preserve student's privacy since it requires them to prove that they are eligible to participate by asking them to authenticate themselves. The authentication reveals, at least to the authentication server, their full identity which opens the door to linking their identity to the questionnaire form they fill in on-line. These considerations may ever deter students from using electronic course evaluation systems resulting in of paper-based course evaluation means with all their disadvantages (e.g. cost, difficulty in processing and preserving evaluation results, small student participation etc.).

Consequently, the goal of the pilot is twofold: (i) to prove the applicability of ABC technology in a real application environment and (ii) provide the first implementation of an electronic course evaluation platform for universities (and educational institutions in genera) that ensures the participants' privacy while, at the same time, guarantees that only eligible students participate by requiring them to reveal only information that proves this eligibility and nothing else.

To achieve these goals, the pilot system will issue to the students Privacy ABCs attesting that they are students of the University and have registered to the course. These credentials will be stored on smart cards that will be distributed to participating students. Moreover, in order to achieve as much as possible accuracy in the gathered opinions of the students, only students who have attended the course sufficiently many times, beyond a preset threshold (can be set to 0 if all students should participate). Thus, in order to receive *attendance credentials* (one per each student appearance in the lecture room) the students will wave their smart cards close to NFC (Near Field Communication) device (essentially, a contactless smart card reader) installed on a computer located in the lecture room. Thus, the number of class appearances, or class attendance units, of each students is equal to the number of class attendance credentials stored in the card.

At the end of the semester, the students will be able to use the credentials stored on their cards in order to authenticate towards the Course Evaluation System and prove their eligibility to participate in the evaluation of the course. They only prove to the system that (i) they are students of the University, (ii) they are registered to the course, and (iii) they have sufficiently many attendance credentials. Nothing else is revealed about the students at any stage of the whole process.

The students are also expected to give feedback with respect to the usability and effectiveness of the ABC technology. The goal is to gather information that will be useful for ABC technology developers and will result in suitable adjustments of the technology to meet their remarks and expectations. This opinion gathering has not been done before for ABC technologies which were, instead, evaluated on a theoretical basis by their developers themselves or by their peers and not by actual users.

Beyond the pilot, our vision is that, as a result of the ABC technologies and the success of the pilot, educational institutions in general will be able to run their own trusted online course evaluation platform. Moreover, the institutions will be able to organize fully anonymous polling procedures targeted to specific *user groups*. This will be accomplished by verifying the eligibility of the users (using ABC technologies) that are allowed to participate and disallowing users that should not interfere with the polling from participation to avoid (perhaps even malicious) "contamination" of the polling results.

4 eVoting vs. Privacy ABCs

Electronic Voting, or eVoting, techniques have given the opportunity to employ computer systems in order to perform electronically national elections as well as less critical types of opinion gathering from public consultation and discussion fora, with low cost, potential for large participation as well as convenient and fast processing of the election results. Of course, participants' *anonymity* is the common denominator of all these processes as one of the major anchor points for protecting the individual's privacy. In this respect one can argue, rather superficially, that both eVoting techniques and Privacy ABCs cover the needs of all such electronic opinion gathering processes. There is subtle difference between them, however, that goes unnoticed at first sight and may reveal the fact the eVoting *end* Privacy ABC techniques are rather complementary to each other and can potentially be used both in opinion gathering applications. The eVoting techniques focus on allowing a voter to *submit*, securely, a voter's opinion rather than *authenticating* her for eligibility to vote. In this respect eVoting targets the *confidentiality* of the vote rather than authenticating the voters. Voter authentication is accomplished by usual PKI based techniques (using suitably drafted election catalogues) that lead to uncovering fully the voter's identity to the system. To say the least, the system *knows* that a particular voter has cast her vote, a fact that the user might not want to reveal. Privacy ABCs, on the other hand, do not target confidentiality of information but user privacy preserving user authentication. In their context, a user can authenticate herself to an eVoting system without revealing her identity at all, and then proceed to cast electronically her vote, in a confidential manner (i.e. vote is encrypted) using eVoting techniques. Therefore, eVoting and Privacy ABCs target different security requirements and can act complementary in order to support *privacy* and *confidentiality* preserving electronic opinion gathering processes.

Moreover, and with an eye towards enhancing the course evaluation pilot later (beyond the scope of the project), there are situations where knowledge of certain characteristics (or attributes) of individuals' profiles may enhance the conclusions drawn from analyzing only the responses of the individuals to an opinion gathering process. For instance, the ministry of education may initiate a discussion as to whether general entrance examinations at the Universities should be abolished and all students enter at the University schools of their choice, depending on their grades only. Then an discussion result indicating that 90% of the participants support the abolition of general examinations may provide some clue as to what the feelings of society are towards the examinations but a closer examination, according to individuals' profiles, may indicate that only 10% of individuals who are university professors support the abolition and, thus, governmental authorities should be careful in implementing such a radical change without further discussion and elaborations. Moreover, there are also situations where knowledge of characteristics of individuals' profiles may be mandatory. For instance, the ministry of education may want to start a discussion about whether University infrastructures in a country are sufficient for a normal operation of Universities. In order to take as substantiated opinions as possible, the ministry decides to open the discussion only to 3rd, or more, year students and professors, who have had sufficiently many years of university life in order to be in position to judge more accurately the University infrastructures.

Overall, our view is that Privacy ABCs with their selective identity disclosure properties offer new opportunities for conducting more accurate privacy preserving opinion gathering processes using the confidentiality properties (e.g. encrypted vote or opinion) of eVoting techniques.

5 Pilot Operational Environment and Requirements

In this section we will describe the environment in which the electronic course evaluation system operates and the main requirements that must be satisfied in order to ensure user privacy and personal information protection.

5.1 The Operational Environment

The course evaluation pilot system will be used by students of the Computer Engineering and Informatics Department of the University of Patras in Greece. The department is located close to CTI's premises, where the pilot system will be installed, operated, and monitored. Figure 1 shows the pilot's system and network infrastructure. Network security relies, partly, on a pair of firewalls which are connected to a high availability configuration (active-standby, without NAT, with automatic fail-over capability between them). The firewalls appear in between the border router and the internal network, inspecting incoming and outgoing traffic and ensuring protection against malicious attacks. For instance, these firewalls can block suspicious source IP addresses in the case of detected DoS attacks as well as traffic directed towards internal servers. However, they alone cannot block packets with malicious content (e.g. viruses) which are taken care of by other components of the security subsystem.

In addition, a *DMZ* subnet exists in CTI's network infrastructure. A DMZ (which stands for "Demilitarized Zone") is a physical or logical subnetwork that encompasses and publicizes an organization's computing services to an external, untrusted network, most commonly the Internet. The DMZ offers an additional security layer to an organization's local area network and services since an attacker from the outside can only access the DMZ and not parts of the internal infrastructure of the organization. The DMZ contains all the servers, such as web and Virtual Private Network (VPN) servers, that offer public services and and do not have (for security reasons) any connection to CTI's internal network. The VPN servers will allow secure remote administration of the Course Evaluation and the University Registration systems. These systems are also in the DMZ and have their own publicly available services. All http/https requests (which obey access control lists and rules) to these servers pass through the DMZ.

The Course Evaluation system supports several different user groups and roles with corresponding remote access rights: students, professors, and possibly members of the *HQAA* (Hellenic Quality Assurance Agency for Higher Education - the organization responsible for ensuring quality in higher educational institutes). For instance, the administrators can access the DMZ via https/http/ssh/ldap connections from CTI's internal network or, remotely, through the Internet (via VPN connections). CTI's domain controller server authenticates the administrators and then control passes to an AAA (Authentication, Authorization, and Accounting) server that will finally give access to the internal network and the two pilot systems.

Finally, at the perimeter of CTI's network infrastructure a border router exists which is placed between the firewalls and the external network and performs some basic checks on incoming and outgoing network activity, such as *ingress* and *egress* filtering that may be helpful in blocking some Internet-based worms from reaching the firewall. In computer security terminology, *ingress filtering* refers to techniques which are employed to verify that incoming traffic actually comes the originators that the traffic packets claim to be from. Complementarily, *egress filtering* refers to techniques of monitoring and, possibly, restricting the type of outgoing traffic from one network to another. Most commonly, this outgoing traffic may contain information from private LANs which may be maliciously directed to the outside network (e.g. the Internet) and should be intercepted and, perhaps, blocked. This border router also implements some generic access list based control in order to increase the level of security and handle some types of attacks like DoS (Denial of Service) or DDoS (Distributed Dos). Additionally, access control lists are maintained by the two internal routers. Through these lists one can specify which processes can access which system objects, as well as what operations are allowed on the objects themselves.

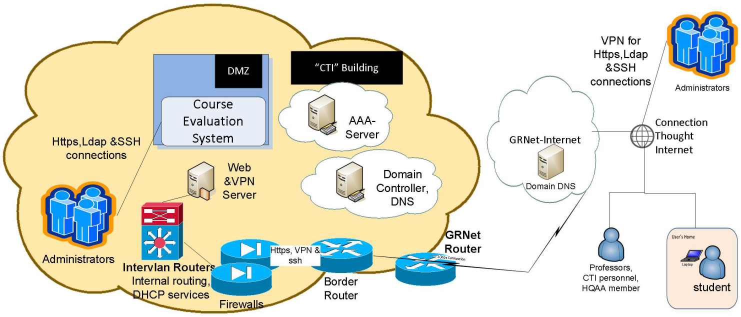

Fig. 1. Course Evaluation System Network Infrastructure

5.2 Pilot Requirements

As electronic course evaluations should be privacy processes, having a focus only on the traditional security requirements, i.e. confidentiality, integrity, and availability ([6]), does not suffice, as it was argued earlier. In the pilot's context, we further need to take care of three additional privacy oriented requirements which are unlinkability, intervenability, and transparency (for further details see [7] and [9]):

- *Unlinkability*: Unlinkability requires that all data processing is done in such a way that the user's actions are unlinkable to each other. Unlinkability is a key element for imposing user data minimization (see [8]) because it encompasses all kinds of separating identity elements from users (i.e. full identity), e.g., by means of anonymization, pseudonymisation, data erasure or simply by not keeping identity data at all. In addition, unlinkability aims at separating different subsets of a user's identity, if they can serve different purposes, thereby supporting the principle of *purpose binding*. Unlinkability, in this wide definition, encompasses the criteria from the Privacy Class in the Common Criteria, i.e. anonymity, pseudonymity, unlinkability (in a stricter definition), and even unobservability in the sense that any observation by another party cannot attest to the action or non-action of a particular user. The main objective of the unlinkability requirement is to minimize risks due to the misuse of user's identity elements and to prohibit or restrict user profiling efforts (see [9]).

However, in some cases there is a requirement for some form of "consumption control" (e.g. one-time coupons, online voting), where users should remain anonymous to the Verifier, but should not be able to use a service more than once by creating multiple, *unlinkable*, identities. This is true in the course evaluation scenario of the pilot where students should not be allowed to participate more than once in the course evaluation. For such scenarios, Privacy-ABCs offer the concept of *scope-exclusive* pseudonyms which are still re-usable but they are unique.

Scope-exclusive pseudonyms are cryptographic pseudonyms derived from a user secret that underlies an issued credential and a scope string (e.g. the URL of a web service). Such pseudonyms are cryptographically guaranteed to be unique per scope string and per user secret. When a Verifier requests from the User to present a scope-exclusive pseudonym for a specific scope, he can be sure that only a single pseudonym can be created per user.

This Privacy-ABC feature is employed in the Patras scenario. When a User (student) interacts with the Verifier (Course Evaluation System), he receives a presentation policy that requests from him to present a scope-exclusive pseudonym with the scope string "urn:patras:evaluation" along with the rest of credential attributes or predicates. This way, a student course evaluation is stored in the system's database along with his scope-exclusive pseudonym. If a student desires to re-evaluate a course, he has to present again his scope-exclusive pseudonym and thus his previous evaluation is overwritten in the database.

- *Transparency*: Transparency requires that all parties involved in any privacy critical data processing operation clearly agree upon and understand the legal, technical, and organizational conditions behind this processing. Satisfying this requirement entails the clear and comprehensible statement of involved regulatory measures such as laws, contracts, or privacy policies, as well as the description of employed technologies, of the organizational processes, and the corresponding responsibilities, among other things. The involved parties parties should understand the risks and have sufficient information on potential countermeasures for privacy regulations as well as on their usage and limitations. This information should be given before the data 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 after the processing has taken place, transparency is required on what exactly happened to the data so that all involved parties can keep record of the processing that took place (for more details see [9]).
- *Intervenability*: Intervenability requires that all the parties involved in any privacy critical data processing operation, including the individual whose personal data are processed, have the opportunity to intervene, where necessary, and interrupt the operation. The goal of this requirement is to offer user corrective measures and counterbalances towards unwanted data operation processes. Intervenability supports the individual's rights to corrective actions and personal data erasure as well as the right to file a complaint or

to initiate a dispute in order to claim amends when undesirable effects have occurred. For data controllers, intervenability allows them to have efficient means to control their data processors, as well as the employed ICT systems, in order to prevent undesirable effects. This includes, for example, the ability to stop a running process in order to avoid further damage, the right to initiate an investigation, ensuring secure erasure of personal data (including data items stored on backup media), manually overriding automated decisions, or applying "breaking glass" policies (for more details see [9]).

These requirements, together with the security requirements we discussed earlier, form a complete set of six user privacy protection requirements. However, as these individual protection goals act complementary to each other, it is possible that sometimes they may act contradictory too. In such a case, an optimum balance should be sought, depending on the application in hand (see [7, 9]).

6 High Level Description of the Pilot System Architecture

The architecture of the pilot course evaluation system is shown in Figure 2. As it can be seen, the architecture is based on various components that have different functionalities and roles. In what follows, we will describe their properties and interactions within the pilot's context.

- *Patras Portal*: This component is web base information portal. Through this portal, the students will get information about the pilot system and functionality as well as information about its usage. Moreover, this portal also contains the necessary links to the components of the system (e.g. University Registration System, Course Evaluation System) that the students should access.

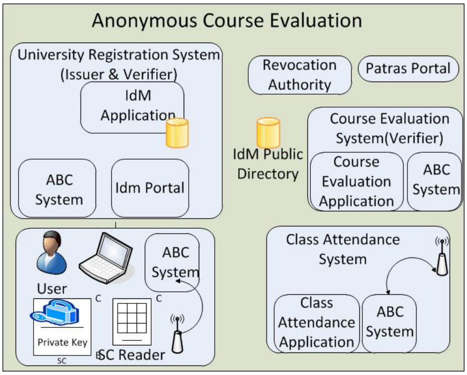

Fig. 2. High Level Architecture

- *University Registration System*: This component issues credentials to the students. It is comprised of the ABC Engine, the IdM (Identity Management) Application, and the IdM portal (the web page that explains to the users how the IdM operates and helps them to create their credentials). The IdM application is a web application whose users are the students and the university registration office employees.

  In particular:

  - A university registration officer is authorized to insert student information in the database of the University Registration System.
  - A university registration officer can revoke a student credential, e.g. when a student graduates from the university or upon student request (e.g. smart card loss).
  - Students are issued credentials that certify that they are, indeed, 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 manage, themselves, a limited subset of their personal information.
  - Students are issued credentials that certify that are registered to the university course that will be evaluated in the end of the semester.

  When a user requests a credential, through the IdM portal, the IdM application invokes the ABC System in order to initiate the issuance protocol.

  Finally, the parameters of the University Registration System (e.g. system parameters, public key information, revocation information) should be stored in a public repository, so that all the other system components can access them. This repository is the IdM Public Directory, as it can be seen in Figure 2.
- *Course Evaluation System:* This component is responsible for the realization of the anonymous course evaluation procedure Its sub-components are an ABC System and a Course Evaluation Application. The ABC System sub-component performs access control to the Course Evaluation Application. This access control is achieved by presenting a policy to the students stating what credentials they must possess in order to proceed. Only users who own the required credentials are given access to the Course Evaluation Application. The Course Evaluation Application is a web application that implements the course evaluation procedure. Potential users of this application are the students, the university professors, and HQAA members.

  More precisely:

  - Course professors can upload questionnaires regarding their courses.
  - Students are able to anonymously evaluate the courses to which they are registered and have attended sufficiently many times.
  - When the evaluation procedure is completed, professors and HQAA members can access the course evaluation results.
- *Class Attendance System:* This component is responsible for issuing an attendance credential to a student's smart card each time the student attends

a lecture. It consists of an ABC System and a Class Attendance software application. The equipment that is required for the Class Attendance System is a laptop with a contactless smart card reader attached to it. The Class Attendance Application runs on the laptop and is responsible for transferring (through the contactless reader) to the students' smart cards the required information during an ABC credential issuance protocol.
- *User's Home Application:* This component needs to be installed on students' personal computers which should, further, be equipped with a contactless or contact smart card reader (if the chosen contactless smart cards support contact operation too). Its main sub-component is an ABC System that enables the user to perform ABC-related operations on their credentials (which are stored in their smart cards) and initiate credential issuance and verification protocols. There is also another software component, called *User Agent*, which is provides the user with an interface that enables her to browse the credentials stored on her smart card, delete credentials and backup credentials on her computer.

With respect to role mapping, the following have been defined:

- *Issuer:* The system component that issues credentials to users. In our pilot this component is the University Registration System. The users of the system, i.e. students of Patras University, interact with this component in order to collect credentials that can be, later, used to prove that they belong to the university and are registered to the course. A second Issuer in our architecture is the Class Attendance System. This component issues an attendance credential to a User, each time she attends a lecture of a course.
- *User:* The entity (human) that collects credentials from an Issuer in order access services offered by a Verifier. The Users in the Patras Pilot are the students that will participate in the trial. In order to interact with Issuer and Verifier components, the students use the User Agent. The User Agent runs locally on their computers and enables them to perform various ABC related operations, e.g. participate in credential issuing and verification protocols as well as use, browse, and delete credentials stored on their smart cards.
- *Verifier (relying party):* The system component offering a service. This component defines restrictions on the credentials that legal users of the service must have and which items from their credentials need to reveal in order to prove their eligibility to use the service. The Verifier accepts credentials from Issuers that she trusts. In our architecture, the component that acts as a Verifier is the Course Evaluation System. This component allows access to a specific course evaluation only to those Users (i.e. students) that satisfy certain properties e.g. students that have booked this course and have attended a minimum number of its lectures. The Issuers that this Verifier trusts are the University Registration System and the Class Attendance System.
- *Revocation Authority:* This component is responsible for revoking issued credentials upon request of the revocation requestor. In our architecture the component that implements the Revocation Authority is the University Registration System. Upon request, a university registration office employee, can

use the University Registration System to revoke the requested credential. Revocation is required in case a student has graduated from the University or when a student loses the smart card containing his credentials.

7 The Realization of the Pilot

We will now take a closer look at the stages involved in the realization of the pilot. We will, first, describe the Setup Phase and how the involved credentials are obtained (i.e. University, Course Registration, and Class Attendance credentials). In addition, we present the basic steps that a student has to follow in order to back-up and restore Class Attendance credentials so as to not miss the opportunity to participate in the course evaluation if she loses her card. Finally, we describe the Course Evaluation process and how student credentials can be revoked.

7.1 System Setup

This section gives a high level description of the generation procedure of pilot and system parameters. The Setup Phase consists of the following steps:

(a) A smart card and a smart card reader is given to each student. The University Registration office provides each student with a smart card in a sealed envelope (which is marked with the corresponding smart card ID and, also, contains the card PIN and a PUK numbers) and a suitably protected slip of paper with a unique student password. In this phase, the smart card does not contain any student information. Furthermore, the slip of paper contains a unique correspondence between the provided smart card ID and the student password. A list of student names and their corresponding identification numbers and passwords is maintained by the University Registration office.

(b) The Course Evaluation System, the University Registration System, and the Class Attendance System are started: The information of students participating in the Pilot (first and last name of the student, University Name, Department Name, and Matriculation Number) is provided to the IdM database by CTI in collaboration with a University Registration office employee. In addition, the administrators of the University Registration System and the Class Attendance System generate issuer parameters and the issuance keys for the involved issuer components. Subsequently, the issuer parameters of the University Registration System are stored in the IdM, so as to he accessible by the ABC System components.

After the above steps have been completed, students install the appropriate software on their computers (e.g. User Agent) and can proceed to the next step in order to obtain their credentials.

7.2 Obtaining University and Course Registration Credential

In order to obtain their University and Course credentials, the students follow instructions provided to them in the Patras portal. These instructions are contained in a User Manual that explains, briefly, the goals and set up of the pilot, the main ABC concepts, as well as the steps that the students need to follow and how they can verify the correctness of their actions. As explained in the manual, each student need to log on to the University Registration System running the IdM. In order to collect a University and a Course credential the student places her smart card into (or near, if the reader is contactless) the reader. After the system has authenticated the student, the credentials issuance protocol is triggered and the generated credentials are transferred in the smart card (see Figure 3).

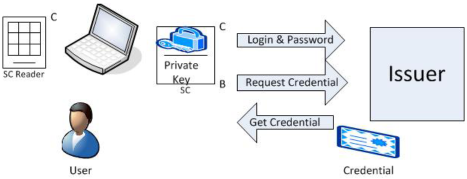

Fig. 3. Obtaining the University or Course Credential

7.3 Obtaining Class Attendance Data

We, will, now describe how a student can collect attendance credentials using the Class Attendance System located in the lecture room. At this point, it is assumed that the System Setup procedures have finished successfully and students have obtained their University and Course credentials.

Fifteen minutes before the lecture begins, an authorized CTI employee will place the Class Attendance System in the lecture room. The Class Attendance System contains the course specific information given by the lecturer (this information includes room number, lecture date, and lecture start/finish times). As soon as the student enters the lecture, she waves her smart card in front of the Class Attendance System in order to collect an attendance credential. This is done by the execution of a credential issuance protocol between the smart card and the Class Attendance System. The generated attendance credential is stored in the card.

Each student can, also, back up attendance credentials and browse the credentials stored on her smart card by running an application locally on her computer (User Agent application). Moreover she will be able to restore the backed up information in case the smart card is lost.

7.4 The Course Evaluation

The pilot involves two rounds, in each of which one course will be evaluated. One round will take place after the end of Fall 2012 semester and the other round will take place after the end of the Spring 2013 semester.

The eligibility criteria, and the corresponding credential verifications, for participating in the evaluations are the following three: (i) the student has a University Credential (i.e. the student belongs to the University) (ii) the student has a Course Credential (i.e. the student has registered the course), and (iii) the student has sufficiently many course attendances (i.e. she has gathered in the smart card sufficiently many attendance credentials). All these criteria are checked for each in a privacy respecting fashion using the ABC technology. In what follows, we describe the course evaluation scenario preparation and execution.

Near the end of each semester, the course evaluation questionnaires are prepared for each course in collaboration with the course lecturer and uploaded in the Course Evaluation application. After the end of the semester, and for a strictly specified evaluation course period, students log on the application and provide, anonymously, their evaluation, after their eligibility is verified according to the three criteria mentioned above. It should be stressed here that each student is allowed to access the Course Evaluation server and provide her evaluation several times. However, only her last evaluation is taken into account due to the use of scope-exclusive pseudonyms (see the discussion on scope-exclusive pseudonyms in Section 5.2).

The Course Evaluation application contains a database for storing eligibility policies and course evaluation data for subsequent analysis. As an important privacy enhancement, the system is configures in such a way that if the employed student eligibility policy for a specific question leads to the emergence of a small and, thus, potentially identifiable subset of students, then the system prevents the student to proceed with this question.

7.5 Student's Privacy-ABCs Revocation

Under certain circumstances, the University registration officials should be able revoke students's credential. This is especially needed in the case a student graduates or finishes a course as well as if her smart card is lost or damaged. In the cases of graduation of course completion, the University Registration System Administrator revokes the credential and eliminates the corresponding information from the university system. In the second case, after the student officially declares smart card loss, the administrator revokes the student University credential and deletes her private information from the ABC system. Subsequently, the student gets a new envelope (containing PIN, PUK) and a smart card form the University Registration office, which she can use to obtain, from the beginning, University and Course credentials in order to restore backed up attendance credentials from her computer (in case she has already performed a back up).

8 Beyond the Pilot

CTI's vision is to be able to extend the ABC4Trust pilot scenario to a full-fledged environment for supporting public consultation and discussion fora targeted at specific educational community groups. The vehicle for this will be the *Greek School Network*, which CTI manages, that connects all Greek schools' local networks together as well as with the Internet. Members of this large community, equipped with ABC based iIdentity cards, will be able to prove their participation eligibility by uncovering the elements of their identities which prove their eligibility in a way that does not uncover their full identity.

The next step is for CTI to promote the use of this consultation environment by the Greek government for enhancing eParticipation in Greece based on gradual introduction of ABC4Trust technology in a small number of Internet based interactions between the citizen and the government and then extend ABC-based privacy preserving services to a wider spectrum of applications useful to the citizens thus contributing to the gradual enhancement of eParticipation and eIdentity management in Greece.

Acknowledgements. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

References

1. Project Description, ABC4Trust-Attribute-based Credentials for Trust, `https://abc4trust.eu/`
2. European Network and Information Security Agency, Privacy Features of European eID Card Specifications. Position Paper (February 2009), `http://www.enisa.europa.eu/act/it/privacy-and-trust/eid/eid-cards-en`
3. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
4. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
5. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Commun. ACM 28(10), 1030–1044 (1985)
6. Federrath, H., Pfitzmann, A.: Gliederung und Systematisierung von Schutzzielen in IT-Systemen. Datenschutz und Datensicherheit (DuD) 24(12), 704–710 (2000)
7. Hedbom, H., Schallaböck, J., Wenning, R., Hansen, M.: Contributions to standardisation. In: Privacy and Identity Management for Life, pp. 479–492 (2011)
8. Pfitzmann, A., Hansen, M.: 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`
9. Zwingelberg, H., Hansen, M.: Privacy protection goals and their implications for eID system (2012)