Privacy Respecting ICT Innovations in Education: Electronic Course Evaluations in Higher Education and Beyond

Yannis C. Stamatiou

Privacy respecting ICT innovations in education: electronic course evaluations in higher education and beyond

Yannis C. Stamatiou[1,2]

[1] Dept. of Business Administration, University of Patras, Patras, Greece,
stamatiu@ceid.upatras.gr
[2] Computer Technology Institute and Press ("Diophantus"), Patras, 26504, Greece

Abstract. In this paper we present our institute's vision towards the introduction of privacy respecting innovative ICT services in the Greek educational sector and, gradually, to other sectors of public interest as well. This vision was shaped during our work within the scope of the EU funded research project ABC4Trust in which our institute implemented a pilot system, based on Privacy-ABCs (Attribute Based Credentials) for the support of anonymous course evaluations in Universities. Privacy-ABCs support cryptographic primitives and tools for eIdentity management that allow users to take full control of what personal information they reveal towards the services they use, providing only the information required to satisfy the service policy. We, first, discuss the set-up of the ABC4Trust pliot and then we explain how we plan to extend the pilot scenarios and characteristics in order to boost eParticipation of members of the educational community of Greece, through the Greek School Network (GSN), in a privacy respecting manner. In particular, we discuss a number of scenarios in which Privacy-ABCs play an important role in ascertaining that users of the GSN only reveal their identity elements which are necessary in order to use a school service. Finally, based on the experiences gathered from our pilot, we present our views with respect to the factors that can inhibit or advance the widespread use of innovations, such as the Privacy-ABCs and the systems based on them, in society. We argue that there are two key factors that affect widespread adoption of innovations: (i) initial introduction of the innovation within groups whose members are linked, somehow, with each other and (ii) gradual introduction to more user groups, of progressively increasing size. This was the model the ABC4Trust project actually adopted in the case of the pilot we discuss in this paper.

1 Introduction

The widespread use of *personalized services*, i.e. services that ask for personal information about users and then process this information or tailor themselves according to users' characteristics has increased, considerably, over the past few years. Such services are, most often, e-Commerce services that address individuals' needs for products based on their buying history as well as the personal information that they voluntarily provide in web forms. Beyond e-Commerce,

social media applications, where revealing personal (even sensitive) information is exactly what they all are about, are gaining increasing popularity, especially among young people.

As a consequence, personalized services, along with their corresponding security and privacy issues, have attracted much attention from researchers in the ICT security domain. Numerous research and survey papers have appeared over the last few years studying various aspects of privacy and privacy preserving authentication mechanisms (see, especially, the publications and work programme of the *Digital Enlightenment Forum*). The discussed aspects include the design of privacy preserving authentication cryptographic primitives, methodologies for verifying, formally, security properties of systems, legislation related to privacy and personal information handling by services as well as the development of new, attractive services whose behavior is determined by personal information items provided by users. Two seminal works (among other similar ones) that, in our opinion, provide an excellent, condensed perspective on the Personal Data Ecosystem and its facets are [10] and [11]. Ann Cavoukian in [10] stresses the role of the individual in handling own personal information and builds the framework for empowering people to handle their own electronic identities in the Web. In [11] Mireille Hildebrandt considers the role of the (digital) environment of the individuals in profiling their habits and actions in order to offer them better personalized services and adjust itself according to their needs. The author discusses the privacy issues arising from this profiling as well as the pros and cons. On the lower level of the PDE, that of cryptographic primitives on which one may build the services and functionalities as described in [10, 11], Florian Kerschbaum in [12] discusses the main cryptographic tools that need to be considered for future privacy preserving and secure Web services.

Privacy Attribute-Based Credentials or Privacy-ABCs, which are described briefly in Section 3, is a technology that enables *privacy preserving*, partial authentication of users. Privacy-ABCs are issued just like normal electronic credentials from a PKI using a secret signature key owned by the credential issuer. However, the distinguishing feature of this technology is that the user can transform his/her credentials into a special *presentation token* that reveals only the personal information which is required by the service policy and nothing else. The verification of this token is performed with the issuer's public key. The *ABC4Trust project* aims at eliminating the gap between theory and practice in Privacy-ABCs 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 the following: (i) to propose an architectural framework for Privacy-ABC technologies that allows their co-existence and interchangeability, and (ii) to provide a *reference implementation* of those ABC components

for potential adopters who wish to incorporate them into their own systems and services. One of the key features of the project is the provision for two pilots, as proofs of concept for Privacy-ABCs: one pilot that involves pupils of a primary school in Sweden and one pilot than involves students of a University in Greece.

In Section 4 we will present, in some detail, the key elements of the pilot, after giving a brief profile of our institute in 2, and will discuss how it served the ABC4Trust project's goals. However, our paper is not limited to only this discussion. Our aim is to present our plans about future extensions of the pilot scenarios and system in order to support safe and privacy preserving services in the educational community in Greece, through the *Greek School Network* that CTI operates and controls, which we describe in 5. Then, taking as a starting point our experiences from running the pilot with a focus on maximizing acceptance of Privacy-ABCs among the pilot participants and beyond, we make an attempt towards generalization: we propose in 6 a generic strategy for introducing Privacy ABCs as well as similar innovation to large user targets by implementing, in a step-wise manner, pilots that involve increasingly larger number of users and provides increasingly complex services. We believe that his *innovation diffusion* strategy may be more effective and efficient in convincing potential users of the usefulness and privacy properties of a service than an abrupt, maybe even by law-enforcement, attempt to introduce the service within large and unrelated user groups right from the start, as it was attempted before by other innovations such as eVoting, with the well-known negative consequences for the innovations. Finally, we conclude in Section 7 with a summary of our findings and pointers to issues for further investigation.

2 The Computer Technology Institute and Press - "Diophantus"

The Computer Technology Institute and Press-"Diophantus" is a research and technology organization focusing on research and development in Information and Communication Technologies (ICT). Particular emphasis is placed on education, by developing and deploying conventional and digital media in education and lifelong learning; publishing printed and electronic educational materials; administrating and managing the Greek School Network; and supporting the organization and operation of the electronic infrastructure of the Greek Ministry of Education, Lifelong Learning and Religious Affairs and all educational units. Since its establishment in 1985, and in the past decades of rapid technological development, CTI has actively contributed to many of the advances that today are taken for granted. The Information Society Sectors are the organization's conveying mechanisms of know-how, in turn supporting the Hellenic State's devolvement into the Information Society.

The principal activity sectors of CTI are the following:

- Educational Technology Sector.
- Networking Technologies Sector.
- E-Government Sector.
- Center of Telematics & Applications for regional development.
- Further Education & Training Sector.
- Strategic & Development Policy Sector.
- Computing & Networking Systems Security Sector.

CTI is, today, in the strong position of combining two important elements which are of great importance in realizing the proposed pilot activities: (i) it administers the Greek School Network, and (ii) it participates in a prominent European project, called ABC4Trust, whose aim is to provide a technical and legal framework for privacy preserving, eIdentity management. The Greek School Network (GSN) is the educational intranet of the Greek Ministry of Education, Life Long Learning and Religious Affairs (abbreviated MoE) that interconnects all schools and a large number of educational administrative units and organizations. It is the biggest public network in the country, having the largest number of users, and has been recognized internationally as a remarkable educational network that promotes the introduction and exploitation of Information and Communication Technologies (ICT) in the Greek educational system. Because of its sensitive educational character and the need to protect pupils while accessing the Internet, GSN needs to adopt strong, privacy preserving authentication mechanisms for its users as well as enhance its services towards the educational community based on these mechanisms.

3 Basic concepts of 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. those based on currently employed PKIs) 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.

Research has resulted in a number of different proposals of how to realize anonymous credentials [3, 5, 7] which are based on different number-theoretic problems and also differ somewhat in the functionality that they offer. There are two leading anonymous credentials systems: Idemix (see, e.g., [8, 6, 9]) of IBM and U-prove of Microsoft (see, e.g., [4]). These two systems provide nearly the same functionality, using different cryptographic primitives. With regard to Idemix, it relies, mostly, on the hardness of the strong RSA problem while U-prove relies, mostly, on the difficulty of discrete logarithms. Also, credentials are represented in different formats. The ABC4Trust project is an attempt to unify these two credential formats into one, focusing on interoperability and operation efficiency. Some of the outcomes of this project may be found in [2] (reference architecture and implementation) and [13] (the University pilot system and scenarios).

4 The course evaluation pilot within the ABC4Trust project

The purpose of the course evaluation pilot was to demonstrate some of the basic functionalities of Privacy-ABCs, to prove their applicability in a real-life scenario and to provide early feedback to the project.

According to the scenarios what where defined within the context of the ABC4Trust project, a number of volunteer students attending a class of the Computer Engineering and Informatics Department of the University of Patras had, first, to collect on the smart cards that were given to them credentials in the form of Privacy-ABCs. These credentials were capable of proving, *anonymously*, that they are indeed students of the University of Patras and that they were registered to the course under evaluation. In some sense, the students obtained a *certificate*, but one whose presentation does not reveal *identifying information*, that could prove their studentship as well as enrollment in the course that will be evaluated in the end of the semester.

During the semester, the students attended the course lectures normally. The additional element (as dictated by the pilot scenarios) was that upon entering the lecture room, they received one attendance credit or certificate of their attendance at that day. This unit was recorded, securely, in their smart cards.

In the end of the semester, they had to anonymously evaluate the course using an online, Privacy-ABCs based, course evaluation system. The entities that were involved in the first round of the pilot and their corresponding ABC roles were the following: (i) University Registration System (ABC Issuer & Verifier), (ii) Class Attendance System (No ABC role), (iii) Course Evaluation System (ABC Verifier), and (iv) Students (ABC User).

The students accessed the University Registration System in order to obtain their credentials, proving their studentship and their registration to the course. The Class Attendance System is the system operated in the lecture room through which the students obtained attendance credits on their smart cards. The Course Evaluation System was the system which the students used in order to evaluate, anonymously, the course they had attended. Also, the students had to install an ABC User Client (User Service + GUI) on their computers in order to be able to interact with the pilot system components. As soon as the pilot started, we provided the students with an envelope containing a properly initialized smart card and the card's PIN and PUK values. We also gave to each of them a contact smart card reader and a slip of paper containing a one-time-password for the initial logging in the University Registration System. The first step for the students was to log in the University Registration System using their matriculation numbers as usernames and their one-time passwords. Then, they were able to register their smart cards so that the University System could link their smart cards with the students' information residing in the system database. After a student had registered his smart card, he was able to obtain the University and Course credentials from the University Registration System. The University credential proves the studentship of the participants and includes, as attributes, his first and last names, the name of the University (Patras University), the Department name (Computer Engineering & Informatics Department) and finally his matriculation number. The Course credential proves that the student is registered to the course under evaluation. In order to be able to evaluate the course in the end of the semester, the students had to collect a minimum amount of attendance credits at the lecture room during the semester. This was accomplished through their interaction with the Class Attendance System. This system, which was operated and supervised by senior personnel of CTI, was located on desk, near the entrance of the lecture room. The students, upon entering the lecture room, had to wave their smart card in front of the contactless SC reader of the Class Attendance System. This action would trigger the execution of a secure protocol between the smart card and the Class Attendance System at the end of which the attendance credit counter residing in the SC was increased by 1. If the student attempted to obtain, illegally, one more attendance credit by waving the SC once more, during the lecture (or, in general, during the same day), then the SC soft-

ware would block the increase operation. In the end of the semester, the students could access the Course Evaluation System in order to evaluate, anonymously, the course they had attended. The presentation policy of the Course Evaluation System asked from the users to prove the possession of a Course credential as well as present a scope-exclusive pseudonym bound to the same secret as the Course credential. The student's SC permitted the participation in such a proof, only if the attendance credit counter in the card was above the preset attendance threshold. Finally, the User Client module (ABC User + GUI) installed on the students' computers offered some additional SC related capabilities. With them, the users could browse the credentials stored on their SCs, change their SC PIN number or unlock it using the PUK value. Moreover, the students could backup and restore the contents of their SCs. This functionality was useful in cases of SC loss or damage so that the user would not lose his attendance credits.

5 Beyond the ABC4Trust pilot: the Greek School Network and the envisaged pilot extensions

The *Greek School Network*, or GSN for short, is the educational intranet of the Greek Ministry of Education and Religious Affairs that interconnects all schools as well as numerous educational administrative agencies and organizations. It is the largest public network in Greece, with the largest number of users, and has been recognized internationally as a remarkable educational network that promotes the introduction and exploitation of Information and Communication Technologies (ICT) in the Greek educational system.

Because of its crucial educational role and the need to protect students when they access outside sites, the GSN applies strong use site and user certification methods. Depending on their access rights and roles, the GSN entities and users belong to one of the the following groups: (i) School units, which are provided with multiple accounts to access the network and the GSN services. (ii) Administrative offices, which are also given one or more accounts. (iii) Teachers who are offered personalized services. The identification process for teachers is provided through an automated environment. (iv) Students, who are given access mainly through the school laboratories, but are also provided with personalized services. The identification of the students is performed directly from their schools, with the collaboration of school administration software and GSNs LDAP service. (v) Administrative personnel, who have access through their schools or offices, and are also provided with personalized services.

The number of connected units is, currently, 16.620 schools and 925 administration units. Broadband penetration exceeds 93% for secondary schools, 73% for primary schools and 30% for kindergartens. The number of teachers that

have a personal account with GSN is, approximately, 77.000 while the number of students is about 51.000. There is, also, a particularly high demand for telematic services, especially email, emailing lists, websites, blogs, educational video streaming, as well as of social networking and e-class services. In particular, the number of active email boxes exceeds 135.000, while more than 9.000 educational websites are hosted in GSNs servers. Also, 3.515 digital courses have been developed by 890 schools (current school year). More than 10.000 educational blogs and 100 educational communities are provided by GSN, and are visited by more than 150.000 unique visitors per month. Finally, the GSN portal is the most highly visited educational portal in Greece, with more than 220.000 unique visitors in a typical month. All the above data have been recorded as of 23 May 2011.

In all the scenarios that follow the underlying principles that will be implemented are: (i) pupils retain their anonymity (unless it is not permitted by specific service policies, e.g. issuance of an attendance credit) while proving other characteristics of themselves (only the elements required by services, nothing else), (ii) pupils and parents are notified (depending on previous agreement between parents and authorities) when and how pupil information is used by authorities with explanation of the reason for this, and (iii) there is provision for using the pupil information discretely, especially health information which should be accessible by authorities in order to extract useful demographic as well as health aggregate information, which implies the implementation of secure storage and querying mechanisms.

5.1 Scenario 1

1. The pupils are equipped with smart cards with ABC credentials that certify that they are pupils as well as other personal information such as matriculation number, age, grade etc.
2. Pupils are registered at the school they are attending in the beginning of the school year by the school registrar. This process is paper based up to now and even in cases of electronic support, the information remains local and out of reach by education authorities.
3. Special credentials are issued to pupils that certify that they have passed the required health exams or at which health aspects they fail. These health certificates are now paper based and their contents are not transformed in electronic format. Thus, the authorities fail to obtain a global view of the health status of the Greek pupil community while, at the same time, severe privacy problems arise.

4. The pupils can order their books at the beginning of the school year using their credentials. Moreover they can download electronic books, which are available by publishers online to certified users, their credentials.
5. Wherever attendance is required, their smart cards can collect it. In this way, the school principal can keep track, for each pupil, the number of times he/she is absent from school and take appropriate measures when needed.
6. Pupils can order and pay their lunch using their smart cards. The smart card contains information about health problems caused by specific foods and, thus, pupils are restrained from consuming specific types of food which danger of unhealthy for them.
7. They can have access to school premises (indoor gym, library, craft classes) after school hours. Their use of the premises can be certified by their personal information will not be revealed if not necessary.
8. The pupils can, also, evaluate (evaluations are totally absent in Greek schools) informally and in an anonymous way the following:
   - School lessons.
   - Teacher notes.
   - Course books.
9. Pupils can certify themselves and watch supporting online courses and classes.
10. Pupils, teachers, and parents will be given the opportunity to discuss and communicate through a special public area offered by the GSN. Today they use, possibly dangerous, online tools, social networking sites, and discussion blogs that may severely compromise their privacy. Privacy preserving technologies can assure, also, that only eligible (according to age, profession, sex etc.) participate in the various chat areas.

In the envisaged scenarios parents are, also, equipped with SCs that verify that they are, indeed, parents of pupils as well as some other personal information of interest to the educational system. Eligible parents can be informed (either automatically or by the school principal) about absences from classes of their children, school activities their children participate in, possibly inappropriate behavior of their children as well as pupils' grades and progress.

5.2 Scenario 2

This scenario includes the basic characteristics of the previous one. In addition, it can include some safety and privacy properties like using ABC technology for authenticating pupils and proving some of their attributes in order to have access to specific web sites and applications:

We can develop an application tuned for use on pupils' laptops and on school lab computers. This application can verify the users through Privacy-ABCs based authentication according to their roles but without requiring identifying information, such as surname. The basic roles are the following:

1. Pupils: No access to web pages with illegal content but access to school services such as like school chat rooms, School forums, the educational material which is uploaded on the Greek School Network etc.
2. Teachers: They can access various GSN services such as discussion fora for teachers only or for parents and pupils, public educational discussion forums, the educational material which is uploaded on the Greek School Network by all other teachers (e.g. supplementary material or solutions to homework assignments) etc.
3. Parents: They can access a variety of GSN services, such as discussion forums where teachers can, also, participate and exchange views with them, parents only discussion forums, the educational material which is uploaded on the Greek School Network etc.

6 What can, potentially, inhibit (or advance) the widespread use of technological innovations such as Privacy-ABCs?

Over the last decade, we have witnessed unprecedented advances in software as well as hardware design and implementation. Especially in the field of security, the advances in theoretical cryptography as well as the construction of highly secure, tamper-resistant hardware devices such as TPMs and smart cards are impressive. Consequently, any security threat, such as the ones our team dealt with during the design and the implementation of our pilot system, could be tackled at a satisfactory level with the appropriate amount of care and effort. Moreover, this should be sufficient to enable the widespread adoption of the Privacy-ABCs innovation by people and organizations alike.

At this point, we should clearly state our view that the other pillar, beyond technology and theory, for adoption of security innovations is users' *trust* towards the innovation. While strong ICT security is a necessary condition for successful security systems, as described in the previous sections, it is by no means (unfortunately) sufficient. In what follows we present the components of a step-wise, trust-driven approach towards the adoption of Privacy-ABCs by people, based on our experiences from the pilot.

The approach involves all stakeholders at the same time and is targeted at convincing them of the usefulness and security of the target system. The principal axes of the approach are the following: (i) Proven technological excellence

of the system components. The system should use strong technologies and theoretical primitives. This aspect may be approached using the latest technological advances in ICT security and cryptography. (ii) Use of open source software technologies and publicly available information for maximum transparency and scrutiny. (iii) In field user assessment. After using the system, the users should be asked to evaluate it and provide feedback on its various aspects, such as user-friendliness, efficiency and perceived security. This feedback should be taken into account for improving the system. (iv) Organization of information days before and after system deployment and use. Holding information days before using a system improves users' understanding of its capabilities and operation while information days after the uses have actually used the system help involved people (developers and users alike) understand each other's views and propose improvements on the usability and functionality of the system. These information days should include technical people, normal users, law experts etc.

We will, now, turn to the important role that *social interactions* among users can play in diffusing innovations, such as Privacy-ABCs. As we argued, the lack of trust from potential users can be a major inhibiting factor in making a technologically perfect technology a success. Then one faces the problem of how to convince people to adopt and use this technology. A promising approach is to let them try the technology and see for themselves how good it is, thus removing the trust obstacle. Our belief is that one of the, potentially, most effective ways of introducing the Privacy-ABCs to potential users is to introduce them, initially, to a small group of closely related individuals and then try to introduce them to large numbers of groups of, progressively, larger number of members.

A mathematical result that appears to support this belief is that proved by Young in [15] within the context of innovation diffusion. It is reasonable to regard Privacy-ABCs and their implementation as an innovation, supported by strong mathematical foundations and a carefully implemented, bug-free (to the extend this is possible) reference implementation, to be diffused over a target user population. Within this context, the mathematical results of Young may be applicable. In what follows, we give a brief overview of these results and discuss their connection with our problem achieving widespread adoption of Privacy-ABCs.

Young described in [15] a parameter of social networks (*graphs*, in general) that characterizes the "closeness" of individuals belonging to a social group. According to this parameter, we characterize a set of individuals as *close-knitted* if the following condition holds for every subset of individuals S in the social group:

$$\min_{S' \subseteq S} \frac{d(S', S)}{\sum_{i \in S'} d_i} \geq r.$$

where $d(S', S)$ denotes the number of links between individuals in the sets S' and S and d_i the number of social links that individual i has in total.

This parameter captures, at the same time, two major "closeness" factors for subgroups of the social graph: (i) internal connections (reflected in the numerator of the fraction), and (ii) external connections (reflected in the denominator of the fraction). Then for a social graph to be r-close-knitted, we require the ratio of these two factors to be at least r, i.e. loosely speaking to have strong internal connections and weak external connections.

What Young proved for families of social graphs which have the r-knittedness property is that the time requited for *all* community members to adopt the innovation, given that a subset of them, whose members we call *initiators*, does accept it initially, is bounded and independent from the size of the community. That is, if all the subsets of the community members have strong pairwise links and, at the same time, are weakly connected to outsiders (who may even be negative towards adopting the innovation), then a group of initiators will manage, in the end, to convince all population members to adopt the innovation. We should note, here, that the definition of close-knittedness is a little more complex for graph families, to which the result of Young applies, than the definition for a single graph but it is along the lines of the definition given above.

This mathematical result suggests a way to, successfully, introduce the Privacy-ABCs innovation to large target populations (e.g. citizens of a city or a country). The central idea behind the proposed approach is to introduce the innovation in a *gradual*, *step-wise* manner that involves increasingly larger individual user groups, as potential *initiators*, that are closely knitted, for some parameter r. For example, the Privacy-ABCs system in hand should be deployed, initially, with users forming small groups of closely related individuals, We would like these users to play the role of the innovation initiators. Consequently, in an ideal situation, they should all adopt the innovation in the end after using it. It follows that in order to convince them to adopt the innovation, we should carefully design the use cases and the supporting ICT system so as to avoid any pitfalls that may cause negative feelings and attitude towards the innovation. To this end, it is preferable to deploy the innovation in the least, possible, risky set-up. For instance, we may use simple use cases, avoiding critical or complex scenarios that may either intimidate users or raise (unnecessary) suspicions over the innovation (e.g. financial applications).

The strategy outlined above has a number of positive features, besides convincing potential users of the innovation quality and usefulness. First, it offers the possibility for in-depth testing of the technology and its implementation since the system is used by a small number of people, each time, and with a simple scenario. As the system testing progresses and modifications are done in

the system to correct bugs or enhance functionalities, the next innovation diffusion phase may take place using a group with a number of individuals and, potentially, a more complex scenario. Then, having controllable individual groups (due to their small numbers and coherence) offers the possibility to organize and conduct a thorough evaluation of the pilot set-up and the implementation of the pilot set-up giving the opportunity to improve them before the next pilot trial. As a positive side effect, possible negative findings or mishaps during the pilot, stay within a small number of people and gives the opportunity for subsequent improvements without much bad publicity spreading to outsiders.

The approach outlined above is similar to the approach we adopted for our pilot within the ABC4Trust project as well as the one we followed in the pilot of another project of CTI, the PNYKA eVoting project (see [14]). More specifically, in the ABC4Trust case (as in the PNYKA project) we targeted a relatively small group of university students (about 50) in order to ascertain "closeness" among them (close-knittedness) due the fact that they both move about within the same location and discuss with each other daily, strengthening their pairwise social links. Due to the "closeness" among them and from the mathematical result about diffusion of innovation among individuals forming such social graphs, our hope was that in the end, after the pilot, the majority of students would be convinced of the value of Privacy-ABCs and their potential applications, unless of course something went terribly wrong during the pilot operation, which was not the case. This group of students would serve as *initiators* to diffuse, further, the Privacy-ABCs to other students. Indeed, the overall impression of the participants was, in general, positive (see [1]) the received feedback was taken under consideration for further improvements and enhancements.

Given this successful operation, our future plan is to follow the gradual innovation diffusion approach discussed above to introduce Privacy-ABCs related services into the GSN. As we explained, this undertaking should be performed with care running, first, small scale pilots within one school, then to more schools within a small geographical region, continuing in this way until we reach larger numbers of GSN users. Before the next step, the participants' feedback will be taken into account in order to prepare for the next, larger scale, pilot. We believe that through this process Privacy-ABCs will be, eventually, adopted by the majority of the educational community members in Greece, an accomplishment that could not be achieved (as indicated by failures of other, initially promising innovations) if one attempted to diffuse, all of a sudden, the Privacy-ABCs technology in, say, eIdentity cards to the whole user population of the GSN. To put this view in perspective, we will end our discussion with one example of a notable failure of a very promising innovation: eVoting. Our belief is that eVoting has failed to gain much popularity in the various countries

that it has been introduced because attempts to introduce it were rather abrupt (even enforced by law) and were targeted to extremely large, virtually unrelated groups of individuals, even whole country populations. In other words, eVoting was introduced to groups of individuals that were not close-knitted and it was, thus, difficult or impossible to adopt and further diffuse the eVoting innovation given, in addition, the misconduct and system failures due to careless design and implementations. The negative discussions of these failures by large numbers of users then created an avalanche effect which actually resulted in the spread of the negative attitude over the whole population which used the eVoting technology.

7 Discussion

We would like to conclude with some lessons learnt from our pilot operation within the ABC4Trust project: a) Modern cryptography and ICT security offer all the necessary tools for building trustworthy Privacy-ABCs systems. b) Security sensitive services and systems should be built using formal design methodologies. c) Privacy preserving services and systems should be designed and built with the end-user in mind. All design steps should be thoroughly documented and explained for later scrutiny by experts as well as non-experts. d) In order to gain wider acceptance, privacy enhancing systems (as any other security sensitive system) should be introduced, gradually, to scenarios of gradually increasing criticality, involving gradually increasing numbers of people over a long time span. e) Finally, a positive attitude towards privacy and Privacy-ABCs can be, potentially, shaped early in the educational system by raising awareness in privacy issues through courses that acquaint pupils with the basics of the Internet, its services as well as its dangers and the protection of their privacy.

Acknowledgement

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. Z. Benenson, I. Krontiris, V. Liagkou, K. Rannenberg, A. Schopf, D. Schröder, and Y. Stamatiou. Understanding and Using Anonymous Credentials. *9th Symposium on Usable Privacy and Security (SOUPS 2013)*.

2. R. Bjones, I. Krontiris, P. Paillier, and K. Rannenberg. Integrating Anonymous Credentials with eIDs for Privacy-respecting Online Authentication. *EU Annual Privacy Forum, Proc. Springer Verlag* , 2012.
3. S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. First Edition, August 2000.
4. S. Brands, L. Demuynck, and B. De Decker. A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users. In *Proc. ACISP 2007*, pp. 400–415, 2017.
5. J. Camenisch and A. Lysyanskaya. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In *Proc. EUROCRYPT 2001*, Vol. 2045, pp. 93–118, LNCS, Springer Verlag, 2001.
6. Jan Camenisch, Els Van Herreweghen. Design and Implementation of the Idemix Anonymous Credential System. *Research Report RZ 3419*, IBM Research Division, June 2002. Also appeared in ACM *Computer and Communication Security* 2002.
7. J. Camenisch and Anna Lysyanskaya. Signature Schemes and Anonymous Credentials from Bilinear Maps. *In Proc. CRYPTO 2004*, pp. 56–72, LNCS, Springer-Verlag, 2004.
8. J. Camenisch: Protecting (Anonymous) Credentials with the Trusted Computing Group's TPM V1.2. In *Proc. SEC 2006*, 135-147, 2006.
9. J. Camenisch and T. Groß. Efficient attributes for anonymous credentials. To appear in *ACM Transactions on Information and System Security (TISSEC)*, 2011.
10. A. Cavoukian. Privacy by Design and the Emerging Personal Data Ecosystem. October 2012. Available at: `http://privacybydesign.ca/content/uploads/2012/10/pbd-pde.pdf`
11. M. Hildebrandt. The Dawn of a Critical Transparency Right for the Profiling Era. *Digital Enlightenment Yearbook 2012*, J. Bus et al. (Eds.), pp. 41–56, IOS Press, 2012.
12. F. Kerschbaum. Privacy-Preserving Computation (Position Paper). *Annual Privacy Forum (APF)*, 2012.
13. V. Liagkou, G. Metakides, A. Pyrgelis, C. Raptopoulos, P. Spirakis and Y. Stamatiou. Privacy preserving course evaluations in Greek higher education institutes: an e-Participation case study with the empowerment of Attribute Based Credentials. *EU Annual Privacy Forum, Proc. Springer Verlag*, 2012.
14. C. Manolopoulos, D. Sofotassios, P. Spirakis, and Y,C, Stamatiou. A Framework for Protecting Voters Privacy In Electronic Voting Procedures. *Journal on Cases on Information Technology* **15:2**, 2013.
15. P. Young. The Diffusion of Innovations in Social Network. In *The Economy as a Complex Evolving System*, vol. III, Lawrence E. Blume and Steven N. Durlauf, (eds.), Oxford University Press, 2003.