D7.2 Necessary hardware and software package for the student pilot deployment

Kasper Damgaard(ALX), Hamza Ghani(TUD), Norbert Goetze(NSN), Anja Lehmann (IBM), Vasiliki Liagkou(CTI), Jesus Luna(TUD), Gert Læssøe Mikkelsen(ALX), Apostolos Pyrgelis(CTI), Yannis Stamatiou(CTI)

Editors:	*Vasiliki Liagkou, Apostolos Pyrgelis, Yannis Stamatiou*
Reviewers:	*Jakob Illeborg Pagter, Ahmad Sabouri*
Identifier:	*D7.2*
Type:	*Deliverable*
Version:	*1.3*
Date:	*27/11/2012*
Status:	*Final*
Class:	*Public*

Abstract

In this document we provide the details of the implementation of the Patras pilot system components as well as their API mapping with the first version of the ABC4Trust reference implementation. We explain how these components interact among them as well as with the pilot users. We provide the details of their set-up, initialization, and proper operation within the ICT infrastructure of CTI and the users' personal computers. We also provide the results of a preliminary risk analysis of the pilot system and we give in the Appendix the user manual for the pilot participation of the students, the user consent form as well as the course evaluation questionnaire that will be used during the course evaluation period.

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

Members of the ABC4TRUST consortium

1.	Alexandra Institute A/S	ALX	Denmark
2.	CryptoExperts SAS	CRX	France
3.	Eurodocs AB	EDOC	Sweden
4.	IBM Research – Zurich	IBM	Switzerland
5.	Johann Wolfgang Goethe – Universität Frankfurt	GUF	Germany
6.	Microsoft Research and Development	MS	France
7.	Miracle A/S	MCL	Denmark
8.	NSN Management International GmbH	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

***Disclaimer**: The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.*

List of Contributors

Chapter	**Author(s)**
Executive Summary	Yannis Stamatiou (CTI)
1. Introduction	Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI)
2. University Pilot Context	Vasiliki Liagkou(CTI), Apostolos Pyrgelis (CTI)
3. University Pilot Architecture	Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI)
4. Deployment of User Client	Gert Læssøe Mikkelsen (ALX)
5. Deployment of University Registration System	Norbert Goetze (NSN), Vasiliki Liagkou (CTI), Apostolos Pyrgelis (CTI)
6. Deployment of Class Attendance System	Apostolos Pyrgelis (CTI), Anja Lehmann (IBM)
7. Deployment of Course Evaluation System	Apostolos Pyrgelis (CTI)
8. Smart Card Deployment	Kasper Damgaard(ALX), Gert Læssøe Mikkelsen (ALX), Anja Lehmann (IBM)
9. API Mapping	Hamza Ghani (TUD), Anja Lehmann (IBM)
10. Network Set Up and Operation	Vasiliki Liagkou (CTI)
11. Risk Management	Jesus Luna (TUD)
Appendix A User Manual	Vasiliki Liagkou (CTI)
Appendix B User Consent Form	Eva Schlehahn (ULD), Harald Zwingelberg (ULD)
Appendix C Student’s Questionnaire	Vasiliki Liagkou (CTI)

Executive Summary

In this deliverable we provide the details of the implementation, set-up and operation of the system that will be employed in the Patras pilot of the ABC4Trust project: remote evaluation of courses by University students. The design, implementation, and testing of the pilot system was based on the use cases and pilot requirements documented in deliverables D5.1, D5.2, and D7.1 as well as the first version of the ABC4Trust reference implementation of Privacy-ABCs provided by WP4.

The *architecture* of the pilot system, as explained in the deliverable, is comprised of five main components: (i) the *Identity Management System*, which is responsible for issuing credentials to the students, (ii) the *Course Evaluation System*, which supports the remote evaluation of university courses by eligible students, (iii) the *User Client System*, which allows students to view and manage their credentials, (iv) the *Class Attendance System*, which registers the number of times that students attend a course, and (vi) the *Smart Cards* and *Smart Card Readers*, which are distributed to the students in order to prove their eligibility for evaluating a course based on Privacy-ABCs technology.

In the sections that follow, our objective is to provide the details of the implementation for each of these components as well as their interaction towards the realization of the pilot's use cases. Emphasis is placed in providing practical implementation requirements and describing in detail the necessary hardware, software, and network environment in which these components can operate efficiently.

We also provide the API mapping of the software components to the ABC4Trust reference implementation libraries as well as the interfacing and interactions protocols employed between the various modules.

Moreover, a preliminary risk analysis is provided that was applied to the current configuration of the pilot system in order to identify and rank the potential risks. We also show how we handled the risks through the security measures provided within CTI's premises and network configuration.

Finally in the Appendix, although it does not concern the integral parts of the pilot system, we give the following information that is nevertheless necessary for the appropriate set-up and run or the pilot and its use cases: the user manual, which the students will be consulting during the operation of the pilot, the course evaluation questionnaire, and the user consent form that they have to sign in order to give their consent to participate in the pilot.

Results pertaining to the evaluation of the pilot, the reference implementation as well as the Privacy-ABCs technologies, in general, based on pilot participants' feedback will be documented in deliverable D7.3 by the end of Month 36 of the project.

Table of Contents

Index of Figures

Index of Tables

1 Introduction

In this chapter we give a general overview of the University pilot. Moreover we present the scope and the structure of this document.

1.1 The University Pilot

The University Pilot will take place in the Computer Engineering and Informatics Department of the University of Patras in Greece. A group of 25 students will poll and evaluate the two courses they took and the respective lecturers. While course evaluations have become standard practice at most universities, they are typically either conducted without the use of computers or by independent third parties to protect the students' privacy. The University pilot will allow limiting the rating process to students that have participated in a lecture without revealing the identity of the students. Beyond this example, the pilot also demonstrates a solution to maintain accuracy and credibility in computer-supported polls, for instance in marketing surveys, while still providing the necessary privacy.

The major challenge for the University Pilot 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, the participating students will have to do the following steps in order to evaluate the two selected courses in a way that ensures the credibility of results and preserves the privacy of the students expressing their opinion:

1. All the participating students will have in their possession a smart card.
2. They have to register their smart card.
3. Then any student can be registered at the Computer Engineering and Informatics Department University or be enrolled in a course by using the ABC technology.
4. All the students that will take part in the evaluation can collect their attendance information at each lecture.
5. Each student can back up his attendance information and to restore backed up data on his (new) smartcard.
6. They will prove that they are indeed students of the department offering the course, they are registered to the course under evaluation and they have attended sufficient number of lectures. In order to submit their course evaluation.

1.2 Structure of the document

The purpose of this document is to give a brief description of the developed hard- and software packages for deployment of the University pilot. Initially, it gives a general overview of the university pilot components and architecture. Moreover it provides a detailed description of the chosen technologies, the developed software, tools and necessary hardware that we used in order to implement the subsystems of the University pilot. Furthermore it presents the API mapping of the ABC services for the main functionalities of University Pilot. Finally this document includes a risk management analysis of University Pilot and its network topology.

In this chapter we introduce the University Pilot. In appendix we included the User manual and the User consent form that we have distributed to the students. Moreover in appendix we also present the data flow diagrams of University pilot. The rest of this document is organized as follows:

Chapter 2 presents University Pilot's environment and the basic actors involved.

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

Chapter 4 provides a detailed description of the developed software, tools and necessary hardware that we used in order to implement User Client of University pilot.

Chapter 5 provides a detailed description of the developed software, tools and necessary hardware that we used in order to implement University Registration System of University pilot.

Chapter 6 provides a detailed description of the developed software, tools and necessary hardware that we used in order to implement Class Attendance System of University pilot.

Chapter 7 provides a detailed description of the developed software, tools and necessary hardware that we used in order to implement Course Evaluation System of University pilot.

Chapter 8 provides a detailed description of the developed software, tools and necessary hardware that we used in order to prepare the smart cards of students.

Chapter 9 presents the designed API mapping of ABC services for the main use cases of University Pilot.

Chapter 10 presents the network infrastructure of University Pilot. Moreover it describes the hardware that hosts the subsystems of University pilot and the necessary tools we used in order to set up University pilot’s subsystems.

Chapter 11 presents the results of applying a novel security- and privacy-aware Quantitative Threat Modelling Methodology to the ABC-related stages of the University pilot.

2 University Pilot Context

In this chapter we describe the facilities which host the systems of the University pilot. There are two main sites the Computer Engineering and Informatics Department and the main building of CTI. In Sections 2.1 and 2.2 we describe the environment where all the user groups can have access to the University Pilots subsystems. Finally in Section 2.3 we present all the user groups and their interaction with the pilot.

2.1 University Facilities

The Computer Engineering and Informatics Department has the opportunity to introduce to the participating students and professors via the Course Evaluation System the Anonymous Based Credentials (ABC) technologies and to enable their efficient/effective deployment in practice. This department 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.

The lectures of the two courses will take place at B4 lecture room in B Building (see Figure 1) which is the main building of Computer Engineering and Informatics Department. All the lecture rooms are accessible to all students of the Computer Engineering and Informatics Department. CTI in cooperation with PhD students will be responsible for placing a NFC reader in the lecture room.

Moreover all members of the Computer Engineering and Informatics Department have access to the Departmental Computer Room (Figure 2) that is located at the second floor of the department’s main building. The main lobby area of computer room is about 500 square meters and it is equipped with 112 PCs, 3 iMac's Apple, 3 high-speed printers, smartboard, digital projectors, tables, microphones, screens for projectors, plasma screens. Personal computers operating system is Windows, UNIX / LINUX and MacOS.

The students can access the following digital services by their PC in the computer room:

- DNS services
- Administering user accounts
- Email and Lists
- File and FTP Server
- Security systems, services and network
- Online Presence and Gateway
- Print Management
- Help-Desk, etc.

CTI will setup few PCs that are located in the computer room in order to be equipped with smart cards readers and the User Client Application.

Figure 1: Building B of the Computer Engineer Department

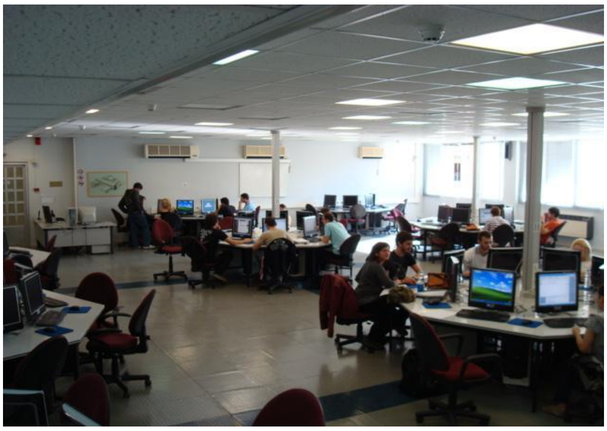


Figure 2: Public Computer Room

2.2 CTI Premises

The subsystems of University pilot will be hosted on the servers that reside on CTI's internal network. The University pilot's systems will be placed in a computer room in the main building of CTI the "D. Maritsa" building at Campus of the University of Patras (see Figure 3). CTI members are responsible for setting up all subsystems of University pilot. 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 border gateway autonomous system. The active network ports in the building "D.Maritsa" are approximately 600. In section 10 we give a brief description of network infrastructure for each University Pilot's subsystem.

Figure 3: CTI building

2.3 User Profile

In the University Pilot there are several groups of users (for more details see section 1.4.1 of D7.1). Students, lecturers, administrators and members of HQAA can access the University pilot via the Internet. More precisely:

- The Course lecturers will be able to access University pilot using their personal computer. They can upload their course questionnaires by establishing an HTTP connection with the Course Evaluation System and by logging on to their accounts using their password.
- Students will be able to access University pilot in order to register their smart card, to be enrolled at department, to backup and restore their SC data, and to evaluate the course. Students can use their personal computer or the computers that are located in the public computer room in order to establish a connection with University Pilot application. Each student could establish an HTTP connection with the Course Evaluation System for evaluating courses, with the Patras Portal for getting instructions and with University Registration System for registering.
- HQAA members will access the University pilot by using login name and password authentication in order to view the accumulated results of course evaluation.
- Administrators can have access to all the sub systems of University pilot by using login name and password authentication in order to add students' information, to administrate the systems, and to process the results of University pilot. Administrators can access all the subsystems of University pilot by establishing HTTPS/HTTP/SSH/LDAP connections through CTI's internal network or the Internet via a VPN connection. One of the administrators will be a CTI member.
- A university registration office employee will not have access to the University pilot, but he can send students' information or a request for revoking a student credential to an administrator.

3 University Pilot Architecture

In this chapter we provide a high level description of the systems that are deployed in the first trial of the University pilot. In Section 3.1 we describe the architecture plan for the full deployment of the pilot as it has originally been designed ([ADFS12]). Subsequently, in Section 3.1 we refer to the essential deflections of the first pilot trial with the full architecture plan. We note here that in the second pilot trial, the overall pilot architecture will be deployed as initially planned.

3.1 Initial Architecture Plan

Figure 4, provides an overview of the components that the pilot architecture consists of. These components have different functionalities and roles based on the scenario and use case definition of this pilot ([DSDBP12]). Next, we describe the functionality and the characteristics of each high level component that is presented on the architecture figure.

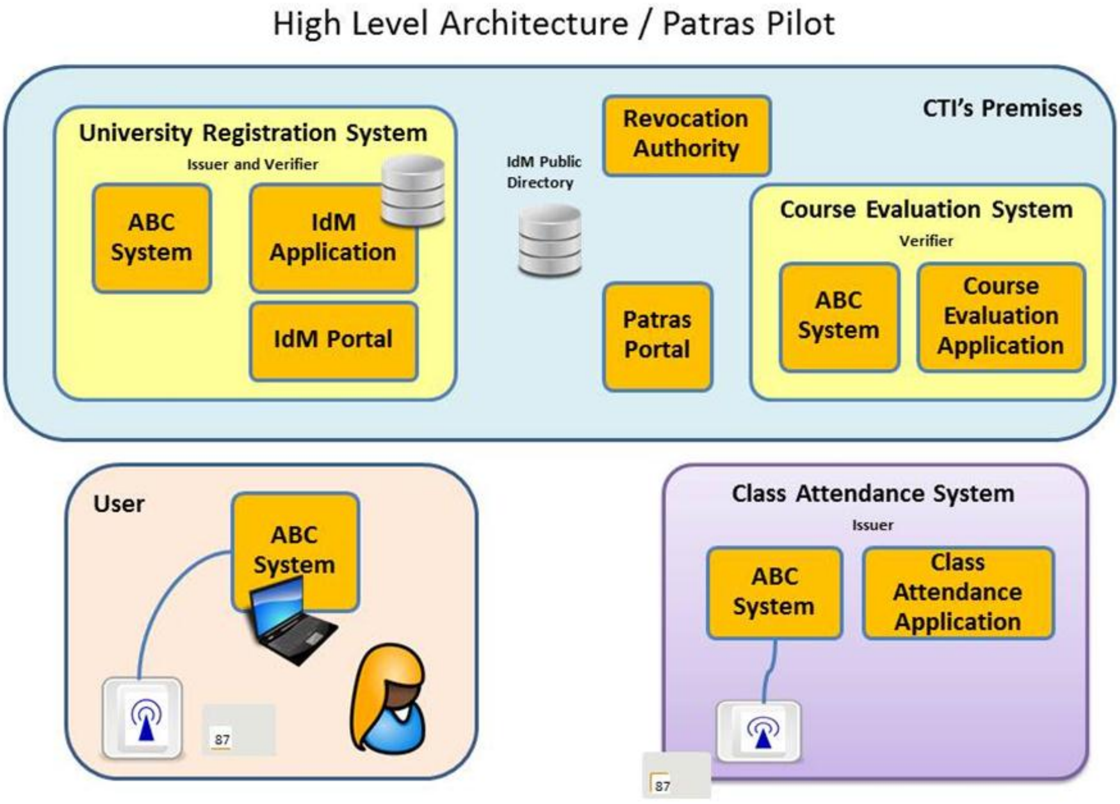


Figure 4 : High Level Architecture of University Pilot

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.
- CTI with collaboration of a university registration office employee has the possibility to register the smart cards that will be distributed to the students that will participate in the pilot.
- 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 that 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 Figure 4.

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 needs. 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 the users with credentials that 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 that will be located in the lecture room of the University and 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 corresponding reader 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. NFC reader's operation will stop 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 University 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 Revocation Authority

In certain cases, a student's credential may need to be revoked. As an example, when a student has lost her smart card, there is the danger of another student that found the card to impersonate the original holder. The student must declare her smart card loss to the University Registration Office. The University Registration System Administrator must revoke the student's University credential and delete the student's private information from the ABC system. Then she can get a new envelope (containing PIN, PUK) and a smart card and re-obtain her credentials.

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.

As depicted on Figure 4, the Revocation Authority is the entity responsible for revoking Privacy-ABCs. The revocation authority has contractual and technical relationship with the Issuer (University Registration System), to know about invalid (and valid) credentials. Further on it needs an interface where revoked credential handles are submitted, as well as an interface the user client can run a non-revocation proof protocol with.

The Revocation Authority publishes its revocation parameters, which contain information about where the Verifier (Course Evaluation System) can check about the latest revocation information and what mechanism to use for this. Revocation information is a set of certified data about the revoked credentials published by the Revocation Authority, which the Verifier uses to check that a certain presentation token presented by a User is not produced by a revoked credential or a combination of them. Depending on the mechanism used, the identifiers of the revoked credentials may or may not be visible from the revocation information. On the other hand, Users also maintain some information about the validity of their credentials, known as non-revocation evidence, which they must update for every credential they possess and against every Revocation Authority listed for that credential.

3.1.5 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.

3.1.6 Patras Portal

This component is an information web portal. Through this portal, the Users can be informed about the “Course Evaluation by Certified Students” pilot. 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 wants 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).

3.2 First Pilot Architecture

In this section we refer to the actual architecture deployment of the first pilot and its deflections with the overall architecture plan. The basic differences of the first pilot architecture with the full deployment architecture plan concern the implementation of the Class Attendance System and the fact that the feature of revocation will not be supported in the first pilot.

3.2.1 Class Attendance System

As it has been described in the project Description of Work, by the time of the first University pilot a first “light” version of smart cards that will support only basic ABC features should be available so that it can be utilized in the trial. That is why we decided to implement a simple approach of the Class Attendance System for the deployment of the first University pilot.

Employing this approach, each time a student attends a course lecture, he waves his smart card in front of an NFC reader available in the classroom and an “attendance counter” on his smart card is increased. When the course evaluation is available at the end of the semester, a student is able to perform an evaluation only if he possesses the required credentials and his attendance counter exceeds a pre-defined attendance threshold (e.g. half of the lectures).

The Class Attendance System consists of an application running on a laptop with an NFC reader attached to it. It is setup by PhD students prior to each lecture with the following lecture identifier. When a student waves her smart card in front of the reader, a communication protocol takes place between the laptop application and the smart card. If the protocol execution is successful the counter on the smart card is increased. Thus, no ABC sub-system is deployed for the Class Attendance System of the first University pilot as no Privacy-ABC issuance takes place. For details of the operation of the Class Attendance System, see Chapter 6. Finally, we note that in the second University pilot, an approach that will support attendance credential issuance from the Class Attendance System will be designed and implemented.

3.2.2 Revocation Authority

The first version of the Reference Implementation ([IRI2012]) was not scheduled to provide an implementation of the revocation feature and thus the first University pilot will not deploy or test revocation. Thus, the entity of Revocation Authority does not exist in the first University pilot. However, the feature of revocation is going to be supported and tested in the second trial of the University pilot that will start on February 2013.

4 Deployment of User Client

This chapter provides an overview of the software and hardware deployment and requirement of the User Client System. On the hardware side the User Client System consists of a smart card storing the user's credentials, and his/her user secret. This makes the system mobile, such that the students do not have to bring anything except the smart card when attending classes, and still later being able to prove attendance. In addition the security of the system is also tightly connected to the smart card. One cannot impersonate the student and rate courses on behalf of others without physical access to the smart card. Interaction with the smart card requires a NFC reader connected to the computer.

On the software side the User Client System consists of the ABC Engine on top of one, or both, of the two Privacy-ABC cryptographic engines (U-Prove and identity mixer). For a full description of the ABC Engine see deliverable D4.1 of this project [IRI2012]. The user interface is done by a Firefox plugin enabling handling of webpages with access based on Privacy-ABC policies.

4.1 Hardware Deployment of User Client System

The only actual hardware of the User Client System is the smart card. The smart card contains special purpose software developed within the ABC4Trust project. More description of the smart card can be found in Chapter 8 of this document. To enable communication with the smart cards each student must be supplied with a NFC reader connected to the user's PC. There are no special hardware requirements except for an Internet connected PC with the smart card reader connected.

4.2 Software Deployment of User Client System

The software consists of two parts: the ABC engine and the User Client Application. The ABC engine is responsible for all lower layers, including handling credentials, smart cards, policies etc. and if possible given the users credentials, providing access tokens fulfilling the requested policies. The User Client is made of a Firefox plugin and an application server executed locally on the user's computer. The User Client is supplying a user interface, making the user capable of choosing between different credentials if more than one fulfils the requested policy. Moreover, in the Patras Pilots, where registration and backup/restoration of smartcards are possible, this is also made possible for the user through the Firefox plugin. An overview of the can be seen below in Figure 5.

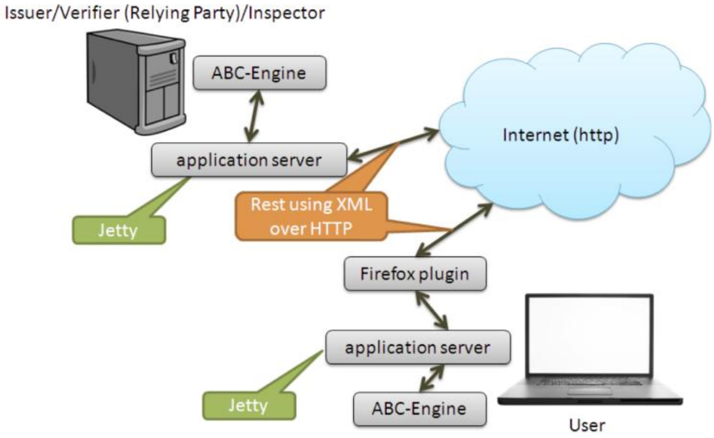


Figure 5: Overview of the software layers <Will be updated to include smart card>

The ABC engine is implemented as a set of web components executed locally on the user's computer, using the Jetty webserver [Jetty] installed locally. For a description of the internal functionality of the ABC Engine see deliverable D4.1 of this project [IRI2012].

The functionality of the user application is also implemented as a locally executed web component using Jetty. The user interface is implemented as a Firefox plugin. This plugin is triggered by tags embedded in the webpages requiring access based on ABC technology, when triggered the plugin sends requests to the user application which will then request the ABC engine for access tokens fulfilling the requested policy. The user interface for backup and restoring the smartcard is also supplied by the Firefox plugin, while the functionality is supplied by the application.

The user side software is packed in on installable package including the Jetty server, the ABC engine, the user application and the Firefox plugin. The requirements for the installation: Firefox, Java 1.6 and in case U-Prove is needed .NET, either the MS implementation or Mono.

5 Deployment of University Registration System

According to the University pilot architecture that has been described in Figure 4, the University Registration System is mainly responsible for issuing credentials to the users. Potential users of this system are students who are able to collect Privacy-ABCs that certify their registration at University and courses that take place there as well as administrators who can populate the system's database with the student attributes, register pilot smart cards or request for revocation of Privacy-ABCs.

5.1 Hardware Deployment of University Registration System

The University Registration System is hosted on two different machines. One is used for the hosting of the underlying ABC System and one for the actual IdM System. Subsequently, we describe the technical characteristics of the two systems.

5.1.1 ABC System

The University Registration ABC System is hosted as a VMware image on an x86 Intel PC equipped with a Xeon CPU 5120 with 2 cores running at 1.86 GHz, offering 4MB of L2 Cache. The University Registration ABC System image has 2GB of memory space available. The available disk space is 40 GB. The IP address of the University Registration ABC System is 150.140.5.76 and its' fully qualified domain name is abce.cti.gr.

5.1.2 IdM System

The University Registration System is hosted as a VMware image on an x86 Intel PC equipped with a Xeon CPU 5120 with 2 cores running at 1.86 GHz, offering 4MB of L2 Cache. The University Registration image has 2 GB of memory space available. The available disk space is 16GB. The IP address of the University Registration System is 150.140.28.70 and its' fully qualified domain name is idm.cti.gr.

5.2 Software Deployment of University Registration System

The project decided to host the University Registration System on 2 different systems (see Figure 6). The reason for this lies mainly in the fact that NSNs IdM is customized for Linux operating systems whereas Microsofts Crypto-Engine (U-Prove CE) requires .NET which itself does not run on natively on Linux.

The University Registration System runs on a 32-bit Ubuntu Linux system, version 10.04 (Lucid Lynx) LTS. Ubuntu is an open source operating system distributed under the GNU General Public License ([GNU GPL]).

The operating system of the University Registration ABC System is a 32-bit Windows Server 2008 standard edition with Service Pack 1.

Adapting the IdM to fit into a Windows operating system would be possible, but this would mean, next to additional customization efforts, that NSNs local test labs and the CTI installation differ in their operating systems which could make debugging more difficult.

The ABCE itself and IBM's Crypto-Engine are java-based applications, which can easily run in a Windows or in a Linux environment.

Instead of hosting all applications on a Windows system, one could consider hosting them on a Linux system. But since there is currently no guarantee that the U-Prove CE can run on Mono (http://en.wikipedia.org/wiki/Mono_%28software%29) without problems, NSN decided to host the entire ABC core components on a Windows system.

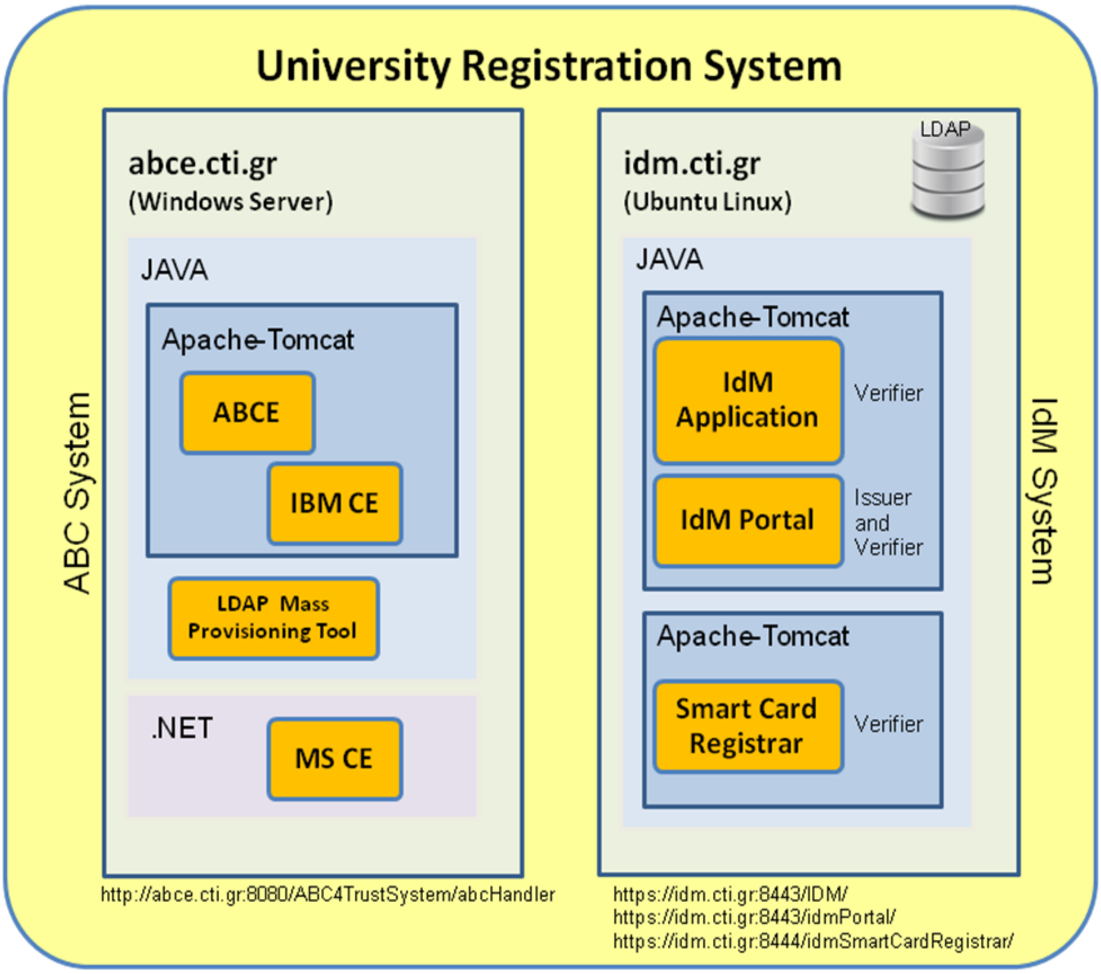


Figure 6: Application Overview of the University Registration System

The host ‘idm.cti.gr’ runs on a 32-bit Ubuntu Linux system, version 10.04 (Lucid Lynx) LTS. Ubuntu is an open source operating system distributed under the GNU General Public License ([GNU GPL]).

The operating system of ‘abce.cti.gr’ is a 32-bit Windows Server 2008 standard edition with Service Pack 1.

5.2.1 Software Deployment of University Registration ABC System

The following programs/applications required for the pilot are installed on the Windows server:

1. jdk1.6.0_35
2. apache-tomcat-6.0.35
3. Microsoft .NET Framework 4.5
4. freeSSHd 1.2.6

5. LDAP Admin 1.1.0.0
6. Microsoft Crypto-Engine
7. ABC4TrustSytem.war web-service (contains the IBM Crypto-Engine and the ABCE)
8. LDAP Mass-Provisioning Tool (java-based)

As can be seen in Figure 6, the ABC System contains an apache-tomcat web server. This server hosts the ABC4TrustSystem web-service, which is configured to listen on port 8080. The IdM System will address this port to proxy all ABC technology related traffic between the User and the Issuer and Verifier ABCE. The ABCE of the ABC System therefore is responsible for handling 2 ABC roles concurrently.

Microsoft's Crypto-Engine is an independent executable which must be 'run as administrator' to listen on port 32123. The U-Prove CE will be addressed by the ABC4TrustSystem web-service in case U-Prove crypto actions need to be performed.

The LDAP Admin program is used to manually inspect and modify the contents of the IdM Database hosted on idm.cti.gr (i.e. IdM System).

For provisioning a larger number of Users, the LDAP Mass-Provisioning Tool facilitates the tasks of the administrator. This tool can read comma-separated csv files and transfer their contents to the IdM database.

Several manual configuration settings were necessary to make the system run. Next to setting the environment variable JAVA_HOME to point to the java installation, the administrator must verify that apache-tomcat is configured to listen on port 8080 by customizing the server.xml file.

For the U-Prove CE, the environment variable 'PathToUProve' must be set to point to the U-Prove executable.

Finally, Windows firewall must be configured to allow traffic to the SSH port and to the HTTP port.

5.2.2 Software Deployment of IdM Portal

The following software has been installed on the Linux system:

1. jre1.7.0_07
2. apache-tomcat-6.0.35
3. LDAP library 2.4-2
4. schemas required by the IdM for the Patras pilot
5. an initial data-set not containing User data
6. IdM application (stored as directory tree)
7. idmPortal.war
8. idmSmartCardRegistrar.war

Contrary to the ABC System, the IdM System hosts 2 instances of the apache-tomcat server. The reason for this is to allow the idmSmartCardRegistrar to listen on a port different to the IdM Portal and the IdM Application. In the Patras pilot, the latter 2 listen on port 8443 whereas the registrar listens on 8444. This way, the network administrators can protect the registrar from unauthorized access from the Internet.

The IdM Application represents the backend of the IdM that authenticates the Users. The IdM Portal is the GUI, which allows Users to inspect the attributes the IdM stored about them. Next to that, Users visit the IdM Portal for registering their smart cards (i.e. 'claiming authorized scope-exclusive pseudonyms)' and for gathering Privacy-ABCs (i.e. credentials).

The IdM Application is basically a SAML server. The IdM Portal a 'trusted third party' of the IdM Application. The IdM Portal uses the IdM Application to authenticate its users.

During the course of the project, the necessity to extract the scope-exclusive pseudonyms from the smart cards and to store them (next to a 'smart card ID') in the IdM database prior to distributing the smart cards to the students became clear. The pseudonyms stored in the IdM database represent a set of authorized values. The reason for this measure is to guarantee that no other smart cards are allowed to communicate with the IdM System. The Smart Card Registrar has been implemented to tackle these tasks.

CTI's network security group must protect the IdM database and the Smart Card Registrar from unauthorized access.

Analogue to the ABC System, the IdM System must be manually configured in several areas. Next to setting the JRE_HOME variable to point to the java installation, the apache-tomcat ports must be customized to use 8443 for the 1st instance hosting the IdM Application and IdM Portal and to use 8444 for the 2nd instance hosting the Smart Card Registrar. Finally, a .keystore file must be stored on idm.cti.gr in order to enable the HTTPS access. The server.xml files of apache-tomcat must be adapted to use the certificate installed in the keystore.

5.2.3 Software Deployment of IdM Application

In order to maintain the University Registration System and to allow Students to access its public web services, CTI's network security group provided some access points (see Figure 7).

SSH, LDAP, RFP (VNC: Remote Framebuffer Protocol), RDP (Microsoft: Remote Desktop Protocol) access points are reserved for authorized administrators only.

HTTPS allows access to public web-services.

And finally, the HTTP access is reserved for communication between abce.cti.gr and idm.cti.gr.

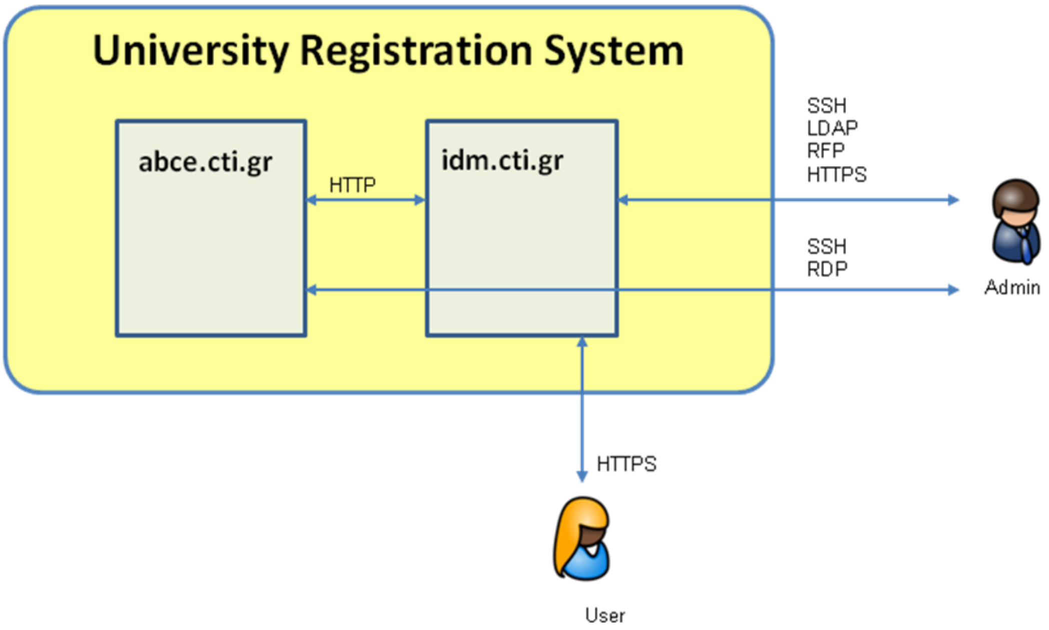


Figure 7: Access Points of the University Registration System

6 Deployment of Class Attendance System

As it has been described in Section 3.1.3 and 3.2.1, the Class Attendance System is an off-line system that students interact with every time they attend to a course lecture. The Class Attendance System is setup offline by CTI engineers with the next lecture identifier. During the lecture, a PhD student places the Class Attendance System in the entrance of the lecture hall. She is also responsible for the operation and physical security of the Class Attendance System. A student who wants to obtain certification of her attendance, waves her smart card in front of an NFC reader and an attendance counter on her card is increased. At the end of the lecture, the Class Attendance System is removed from the lecture hall.

6.1 Hardware Deployment of Class Attendance System

The Class Attendance System runs on a HP laptop (HP Compaq 6720s) with an Intel Core 2 Duo Processor at 1,6Ghz and 1 GB RAM. HP laptop has windows xp operating system with service pack 3.

An Omnikey 5321 smart card reader is attached to an USB port of the laptop. This reader has a dual interface and thus can support communication with both contact and contactless smart cards. For the Class Attendance System we use the RFID interface of the Omnikey 5321 smart card reader.

Figure 8: Omnikey 5321 smart card reader

6.2 Software Deployment of Class Attendance System

The laptop that the Class Attendance System is hosted on, runs the Microsoft Windows 7 operating system. The PC/SC (Personal Computer/ Smart Card) specification is available under Windows operating systems and thus smart card integration into this computing environment is feasible.

When a student waves his smart card in front of the Omnikey 5321 reader, a Java application that is executed on the laptop is responsible for performing a communication protocol between the laptop and the student’s smart card. If the communication protocol is successful, the attendance counter on the student's smart card is increased. The following subsection (6.2.1) describes in detail the communication protocol that takes place between the student's smart card and the laptop.

6.2.1 The Class Attendance Application

Here we give a detailed description of Class Attendance Application, which is developed according the First Pilot Architecture (see Section 3.2). In Section 3.2.1we presented the operation of Class Attendance System for the first trial.

When a student attends a lecture of a course, he is eligible to obtain a certification of that attendance. This certification is done by increasing an attendance counter on a trusted storage space of her smart card. More specifically, the counter can be increased only:

i) once per lecture

ii) when triggered by a legitimate class attendance system

During the smart card initialization phase that is performed by the pilot administrators, the student's smart card is initialized with an attendance counter for the university course. This attendance counter has a specific counter identifier "counterId", an initial index (counter value) set to zero, a threshold value "threshold" and a counter cursor "cursor" set to zero. The threshold value determines the minimum attendance that a student should have in order to be able to participate in a course evaluation. The cursor value is used for storing the last lecture identifier on which the student was present. Moreover, attached to this counter is the public key of the Class Attendance System that has been generated during the pilot setup phase.

Offline, the Class Attendance Application is initialized with a fresh lecture identifier by CTI engineers. The lecture identifiers are strictly increasing for each new lecture. Thus, the lecture identifier is simply 1 for the first lecture, 2 for the second, and so on.

When a student waves his smart card in front of the contactless reader, her card and the class attendance system run the following communication protocol:

1. The student's smart card generates a random nonce "challenge". It sends the nonce to the Class Attendance Application and also stores it locally.
2. Upon receiving the random challenge, the Class Attendance Application produces a signature "sig" on the blob "counterId|| newcursor ||challenge", using the Class Attendance System secret key "sk_cas". The "counterId" is the counter identifier for this course, the "newcursor" is the value of the current lecture identifier and the "challenge" is the value of produced by the smart card in Step 1. (see Appendix of smart card manual for the signature algorithm) :

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

3. Now the smart card attempts to increase by one the counter "index" of the counter with identifier "counterId" by doing the two following checks:
   a. Verify(pk_cas, sig, m) = true for m = counterID || newcursor || challenge
   b. cursor < newcursor (i.e. it sees a fresh lectureID)

The first check takes place in order to verify the authenticity of the Class Attendance System. Specifically, it verifies the signature "sig" with the public key of the Class Attendance System "pk_cas" that is stored in it and using the challenge produced by it in Step 1. The second check is executed in order to ensure that the students counter is updated once per lecture, even if they wave their card multiple times in front of the reader.

If one of the above checks fails, or no counter with “counterId” was stored, the smart card indicates failure towards the card reader. Otherwise, the smart card increments the counter value by one, sets cursor = newcursor and indicates successful counter update towards the Class Attendance Application.

7 Deployment of Course Evaluation System

According to the University pilot architecture that has been shown in Figure 4, the Course Evaluation System is the component responsible for the realization of the course evaluation process. Potential users of this system are certified students who are able to evaluate a course they have registered and attended to, professors who can create evaluation questionnaires for the courses that they teach and HQAA officers who have access to the course evaluation results.

7.1 Hardware Deployment of Course Evaluation System

The Course Evaluation System is hosted as a VMware image on an x86 Intel PC equipped with a Xeon processor 5120 with 2 cores running at 1.86 GHz, offering 4MB of L2 Cache. The Course Evaluation System image has 2 GB of memory space available. The available disk space is 16GB. The IP address of the Course Evaluation System is 150.140.28.71 and its' fully qualified domain name is ces.cti.gr.

7.2 Software Deployment of Course Evaluation System

The Course Evaluation System runs on a 32-bit Ubuntu Linux system, version 10.04 (Lucid Lynx) LTS. Ubuntu is an open source operating system distributed under the GNU General Public License ([GNU GPL]). Both Course Evaluation ABC System and Application are executed on this system. Figure 9 presents an overview of the Course Evaluation System architecture.

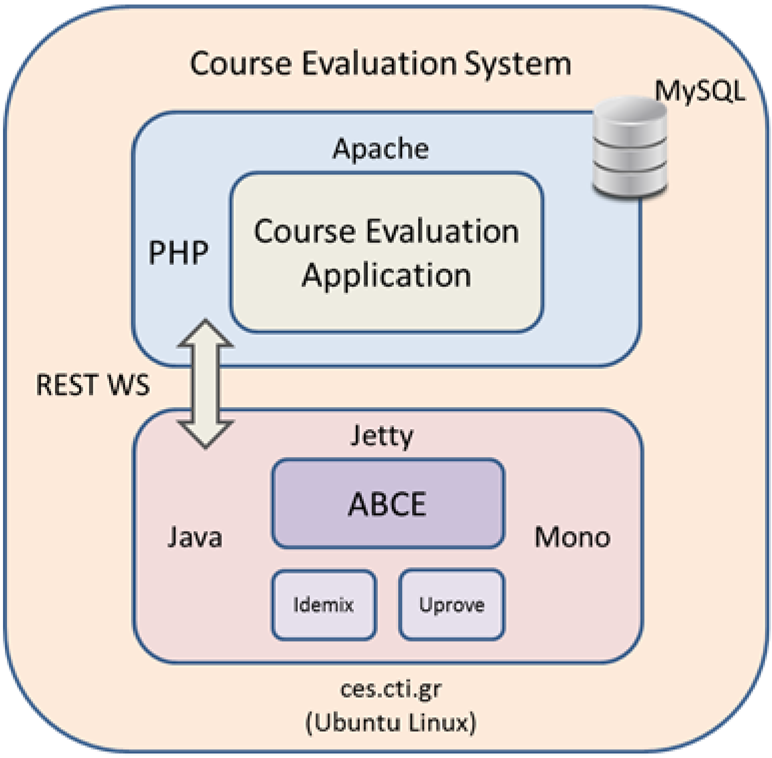


Figure 9: Course Evaluation System Architecture

7.2.1 Software Deployment of Course Evaluation ABC System

In the project's reference implementation (D4.1), the ABC engine of a verifier has been implemented as web components that are exposed to the application layer as web services. Thus, the Course Evaluation ABC System has been implemented as Java REST web services that are exposed to the application layer through HTTP/HTTPS. These web services are running on Jetty ([Jetty]) web server version 7.0.1. Jetty is a pure Java based HTTP server and has been developed as a free and open source project. Moreover, the Mono software platform version 2.10 is deployed on the system in order to execute the U-Prove crypto engine components that have been implemented in .NET/C#.

7.2.2 Deployment of Course Evaluation Application

The Course Evaluation Application is a web application that has been developed with Drupal version 7 ([Drupal]). Drupal is a free and open source Content Management System (CMS) written in PHP and distributed under the GNU General Public License ([GNU GPL]).

Drupal runs on any computing platform that supports both a web server capable of running PHP (including Apache, IIS, Lighttpd, Hiawatha, Cherokee or Nginx) and a database (such as MySQL, MongoDB, MariaDB, PostgreSQL, SQLite, or Microsoft SQL Server) to store content and settings. Drupal 7 requires PHP 5.2.5 or higher. The Course Evaluation Application runs on Apache ([Apache]) web server and the content is stored on a MySQL ([MySQL]) database.

8 Smart Cards Deployment

This chapter describes the management functionalities of the smartcards. These are the initialization of the smart cards, backup of the secure data including the state of collected credentials and counters and the restoring of this data. Class attendance and proofs of class attendance are described in Chapter 3.

The smart cards also provide more advanced functionalities such as firmware update and factory reset, these functionalities are not described here, as they are not intended to be used by the students or other end users of the cards. For a description of these functionalities we refer to the smart card manual [BDP12].

8.1 Smart Cards Initialization

Before being used the smart card has to be initialized with the cryptographic parameters that it has to use. These values include the public key of the issuer, and other cryptographic parameters being used in issuance of credentials and proofs using the credentials. The initialization of the card also includes PIN code generation and key generation inside the card itself.

When initializing the card the first thing being done is putting the card from virgin mode into root mode using an access code which changes with each firmware update of the cards software. Then the root authority generates a cryptographic keypair. These keys are used for making the smart card and the computer capable of sending some secret values securely between the two, and can at later stages also be used for root-authorized commands such as deleting or adding an issuer. For efficiency reasons not all communication is secured, however, all secret values such as PIN, PUK etc. are communicated securely, this is to avoid eavesdropping on the NFC (wireless) connection. After this the smartcard generates a random master secret used for secure issuance of credentials and proofs. A random PIN code and a random PUK code are also generated. The PIN code is used whenever the user wants to use some of the security related functionalities of the smart card. The PUK code is used to re-enable the card if a wrong PIN code has been typed more than three times. The PIN and the PUK codes are sent to the user client and are stored in a file on the root authority computer used to initialize the card.

The smart card is also initialized with a set of cryptographic parameters, specifying which algorithmic groups should be used for computing cryptographic values, and the card is initialized with parameters including the public keys of the issuers, which the card should be able to receive credentials from. In the Patras pilot, this is the University Issuer, issuing the University credential; and the Course Attendance Issuer, issuing Course Attendance credentials. If the smart card is a U-Prove card, then an Identity Mixer issuer has to be added. This is due to the architecture of the ABC engine, where some of the cryptographic functionalities are shared between the U-Prove and the Identity Mixer Crypto-Engines.

The last initialization steps are that the card is changed from being in root mode to be in working mode, and a scope exclusive pseudonym is put on the card to make the card capable of proving that it is the correct card, when later communicated with.

8.2 Backup & Restore

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

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

8.2.1 Backup

prerequisite: student and smart card are already registered at the university registration system.

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

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

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

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

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

The user does not see these three steps, as the user interface just asks him for the PIN once and for a password, and then the user client makes the three calls to the cards, retrieves all the data to be backed up, and stores all data in one backup file.

8.2.2 Restore

When a student has to obtain a new smart card, due to the loss or malfunction of the original one, he can contact a university representative of the pilot with his latest backup and a valid identification document.

The new card must be initialized by the university representative with the same device identifier as that of the previous card. Moreover, the issuers, Provers and counters must also be set. The new PIN and PUK are provided to the student. When the user obtains his new card he can trigger the user client and do the following restore procedure. He clicks on the restore button and selects the archive on his PC to restore on the card. He is asked to enter the new PIN and the password that is associated with the backup archive. If the deviceID is the same as before, the restore takes place and the user now has in his new card the old data (PIN, PUK, deviceKey, counters and credentials).

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

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

b) A mechanism that restores counter specific data (counter id, index and cursor). This mechanism (“RESTORE COUNTERS” command) requires from the user to enter the card PIN as well as the password that was used for backup.

c) A mechanism that restores credentials. This mechanism (“RESTORE CREDENTIAL” command) requires from the user to enter the card PIN as well as the password that was used for backup.

As with the backup the user does not see these three individual steps. Seen from the user there is only one restore command, and the user client does the three calls to the card using the pin of the new card along with the password given when backing up the card.

9 API Mapping

In this chapter we describe the API mapping of the ABCE for the following University Pilot Use Cases. The focus is on the ABCE method calls. The Use Cases have been defined and described in the previous deliverable D7.1 (see section 2.2 of D7.1 [ADFS12])

9.1 System Setup

Table 1 and Figure 10 show the API mapping for the first use case (GR_1: All the parties of the system first need to go through an initialization phase in order to become functional). The interested reader is referred to Section 2.2.3. of D7.1 [ADFS12]

Table 1. ABC System Setup

Step	Explanation
1	The "ABC System Admin" creates the system wide parameters by invoking the ABCE method *setupSystemParameters(keylength:integer, mechanism:anyURI)*
2	The "ABC System Admin" creates issuer parameters and issuer secret key for credUniv (issuerUniv), as well as issuer parameters and issuer secret key for credCourse (issuerCourse): *setupIssuerParameters(credspec:CredentialSpecification, syspars:SystemParameters, uid:anyURI, hash:anyURI, revparsuid:anyURI)*
3	The "ABC System Admin" creates the pilot specific parameters (not related to the ABC Engine)
4	The "ABC System Admin" initializes the smart card by setting the values (not related to the ABCE)
5	The "ABC System Admin" invokes the smart card to obtain a (scope-exclusive) pseudonym and store the returned pseudonym on the IdM database.
6	The initialized smart card is delivered to the student (not related to the ABCE)

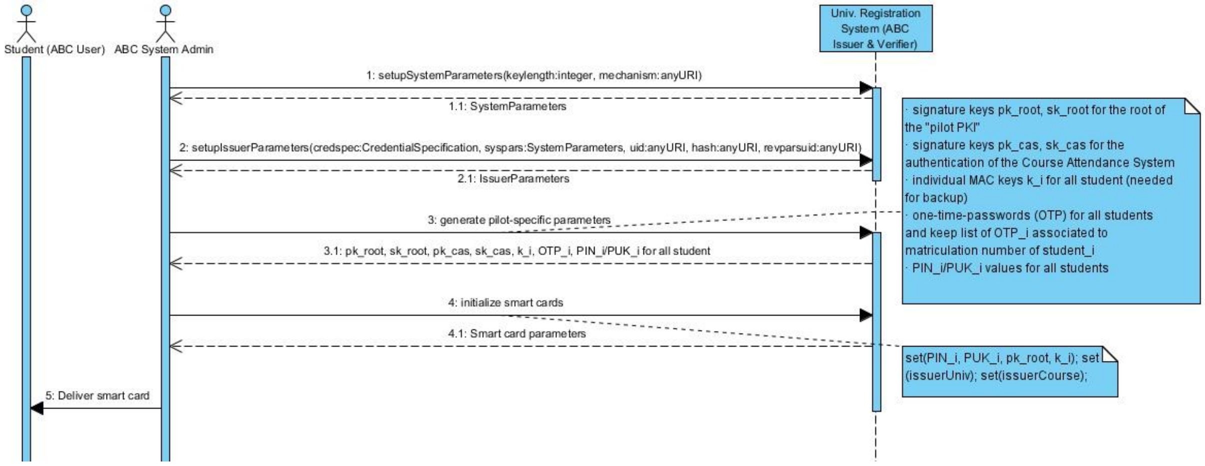

Student (ABC User)
ABC System Admin
Univ. Registration System (ABC Issuer & Verifier)
1: setupSystemParameters(keylength:integer, mechanism:anyURI)
1.1: SystemParameters
2: setupIssuerParameters(credspec:CredentialSpecification, syspars:SystemParameters, uid:anyURI, hash:anyURI, revparsuid:anyURI)
2.1: IssuerParameters
3: generate pilot-specific parameters
3.1: pk_root, sk_root, pk_cas, sk_cas, k_i, OTP_i, PIN_i/PUK_i for all student
4: initialize smart cards
4.1: Smart card parameters
5: Deliver smart card
· signature keys pk_root, sk_root for the root of the "pilot PKI"
· signature keys pk_cas, sk_cas for the authentication of the Course Attendance System
· individual MAC keys k_i for all student (needed for backup)
· one-time-passwords (OTP) for all students and keep list of OTP_i associated to matriculation number of student_i
· PIN_i/PUK_i values for all students
set(PIN_i, PUK_i, pk_root, k_i); set (issuerUniv); set(issuerCourse);

Figure 10: ABC System Setup

9.2 Registration and Login of Students

Here we present the API mapping for the use case GR_2_1. This use case describes the steps needed for a student to get the certificate for registration at the University. For more details about this use case we refer to Section 2.2.4. of D7.1 [ADFS12].

9.2.1 GR_2_1: University Registration

Table 2 and Figure 11 show the API mapping for the use case GR_2_1.

Table 2. Registration & Login of Students

Step	Explanation
1	The student logs in to the university system and authenticates using matriculation number and OTP *Login(matriculation number, OTP)*. She gets *PresentationPolicy PolicyUID="urn:patras:policies:loginPseudonym"*as a return.

2	The student invokes the *createPresentationToken(p:PresentationPolicyAlternatives)* method using the received presentation policy from Step 1 in order to obtain the presentation token containing the requested pseudonym. The presentation policy can be:
	`<abc:PresentationPolicyAlternatives ...>`
	`  <abc:PresentationPolicy PolicyUID="urn:patras:policies:loginPseudonym">`
	`    <abc:Message>`
	`        <abc:Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</abc:Nonce>`
	`    </abc:Message>`
	`    <abc:Pseudonym Exclusive="true" Scope="urn:patras:registration"`
	`Established="true"/>`
	`  </abc:PresentationPolicy>`
	`</abc:PresentationPolicyAlternatives>`

3	The university registration system verifies the token by invoking the *verifyTokenAgainstPolicy(p:PresentationPolicyAlternatives, t:PresentationToken, store:boolean)* method of the ABCE

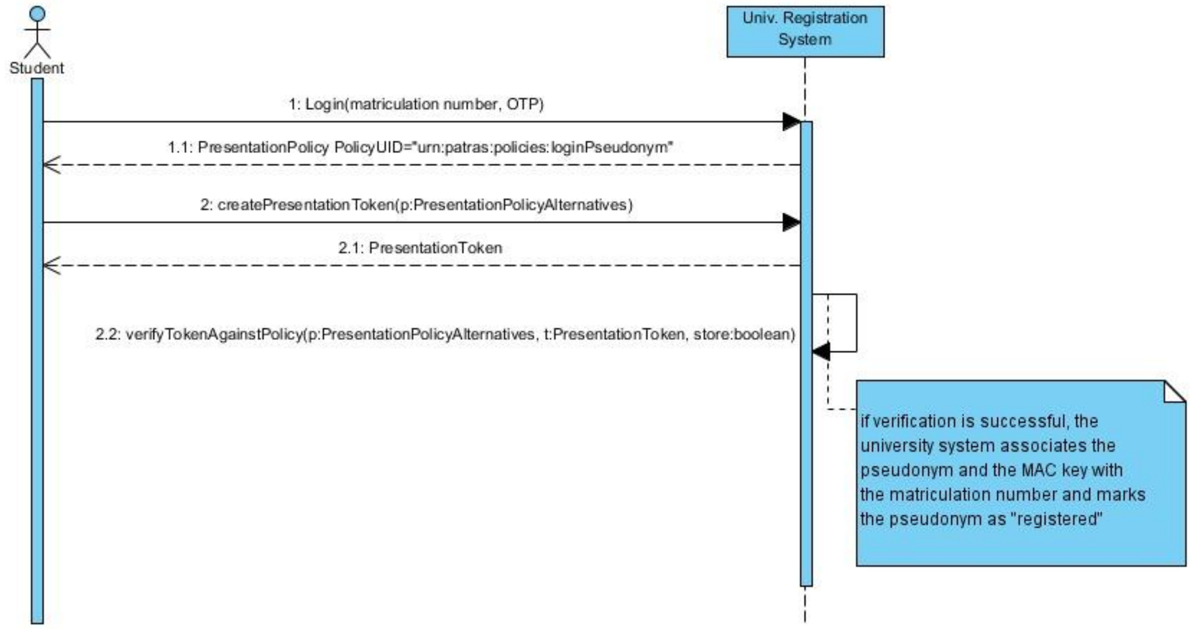

Student
Univ. Registration System
1: Login(matriculation number, OTP)
1.1: PresentationPolicy PolicyUID="urn:patras:policies:loginPseudonym"
2: createPresentationToken(p:PresentationPolicyAlternatives)
2.1: PresentationToken
2.2: verifyTokenAgainstPolicy(p:PresentationPolicyAlternatives, t:PresentationToken, store:boolean)
if verification is successful, the university system associates the pseudonym and the MAC key with the matriculation number and marks the pseudonym as "registered"

Figure 11: Registration & Login of Students

9.3 Obtaining the University and Course Credentials

Here we present the API mapping for the use cases GR2_2 and GR_5. 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. For more details we refer the interested reader to Section 2.2.4 in [ADFS12]).

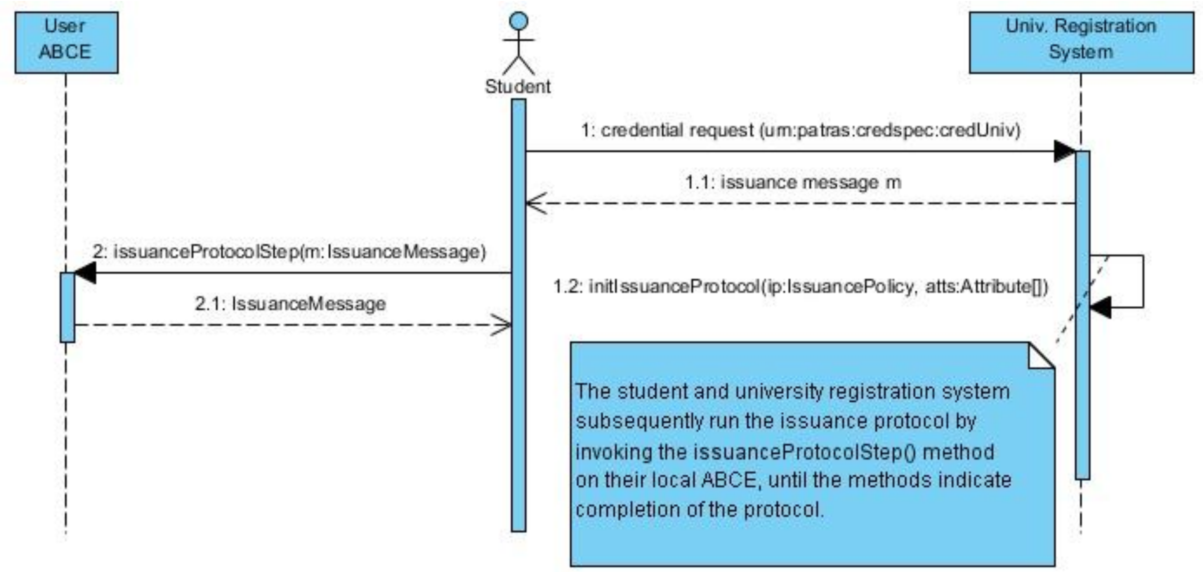
9.3.1 University Credentials

Table 3. Obtaining the University Credentials

Step	Explanation

1	The student sends a credential request for urn:patras:credspec:credUniv.
	The university registration system responds with an issuance message which contains the issuance policy that specifies that the newly issued credential will be bound to the same secret key as the (scope-exclusive) pseudonym that the user has already established. To this end, it invokes the *IssuerABCE.initIssuanceProtocol(ip:IssuancePolicy, atts:Attribute[])* method on input the issuance policy stated below and the known attributes of the student.
	`<abc:IssuancePolicy Version="1.0"`
	`xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0">`
	`  <abc:PresentationPolicy PolicyUID="urn:patras:policies:issuance">`
	`    <abc:Pseudonym Exclusive="true" Scope="urn:patras:registration"`
	`Established="true"`
	`     Alias="#nym"/>`
	`  </abc:PresentationPolicy>`
	`  <abc:CredentialTemplate SameKeyBindingAs="#nym">`
	
	`<abc:CredentialSpecUID>urn:patras:credspec:credUniv</abc:CredentialSpecUID>`
	
	`<abc:IssuerParametersUID>urn:patras:issuer:credUniv</abc:IssuerParametersUID>`
	`  </abc:CredentialTemplate>`

	`</abc:IssuancePolicy>`
2	The student and university registration system subsequently run the issuance protocol by calling the *issuanceProtocolStep(m:IssuanceMessage)* method on their local ABCE, until the methods indicate completion of the protocol. Note: Neither the ABCE nor the presentation policy support a request & check yet that a presented pseudonym in the issuance token is a particular pseudonym, e.g., from another presentation token. In the pilot, this check must be done by the university system itself, in order to ensure that a credential is bound to the same student/card that is logged in. This holds for the issuance of course credentials as well.


User ABCE
Student
Univ. Registration System
1: credential request (urn:patras:credspec:credUniv)
1.1: issuance message m
2: issuanceProtocolStep(m:IssuanceMessage)
2.1: IssuanceMessage
1.2: initIssuanceProtocol(ip:IssuancePolicy, atts:Attribute[])

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

Figure 12: Registration & Login of Students

9.3.2 Course Credentials

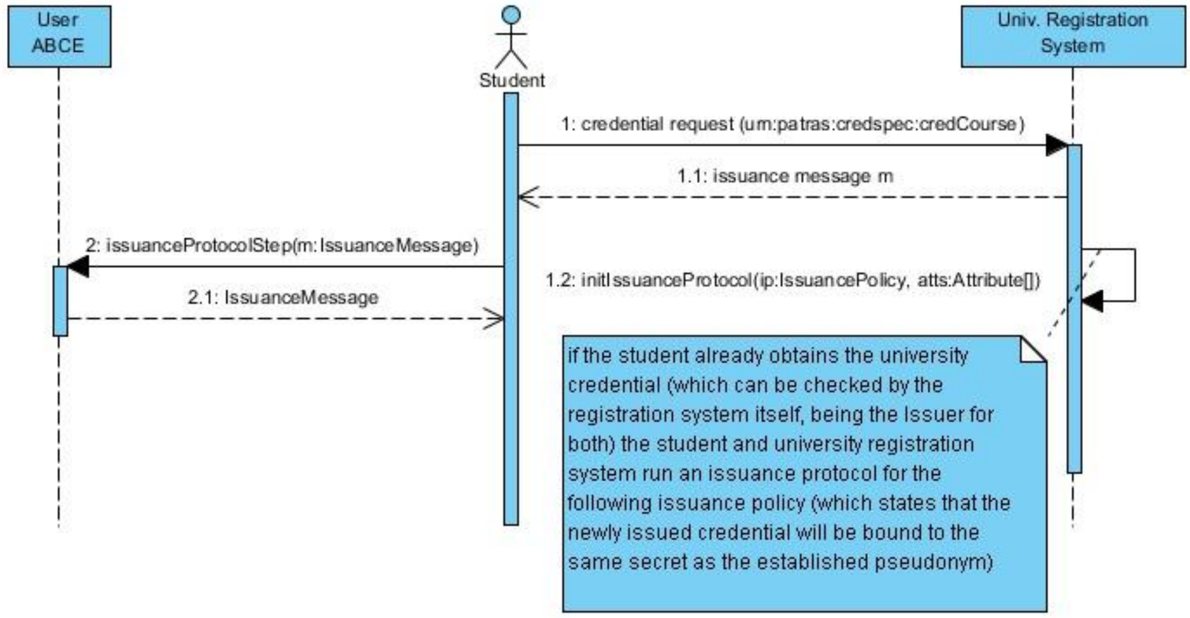
Table 4. Obtaining the Course Credentials

Step	Explanation

1	The student sends a credential request for urn:patras:credspec:credCourse.
	The student and university registration system run an issuance protocol for the following issuance policy:
	`<abc:IssuancePolicy Version="1.0"`
	`xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0">`
	`  <abc:PresentationPolicy PolicyUID="urn:patras:policies:issuance">`
	`     <abc:Pseudonym Exclusive="true" Scope="urn:patras:registration"`
	`Established="true"`
	`      Alias="#nym"/>`
	`  </abc:PresentationPolicy>`
	`  <abc:CredentialTemplate SameKeyBindingAs="#nym">`
	
	`<abc:CredentialSpecUID>urn:patras:credspec:credCourse</abc:CredentialSpecUID>`

	`<abc:IssuerParametersUID>urn:patras:issuer:credCourse</abc:IssuerParametersUID>`
	`  </abc:CredentialTemplate>`
	`</abc:IssuancePolicy>`

2	The student and university registration system subsequently run the issuance protocol by calling the *issuanceProtocolStep(m:IssuanceMessage)* method on their local ABCE, until the methods indicate completion of the protocol. when the smart card recognizes that a course credential is generated, it also triggers the activation of the counter blob on the card.


User ABCE
Student
Univ. Registration System
1: credential request (urn:patras:credspec:credCourse)
1.1: issuance message m
2: issuanceProtocolStep(m:IssuanceMessage)
2.1: IssuanceMessage
1.2: initIssuanceProtocol(ip:IssuancePolicy, atts:Attribute[])

if the student already obtains the university credential (which can be checked by the registration system itself, being the Issuer for both) the student and university registration system run an issuance protocol for the following issuance policy (which states that the newly issued credential will be bound to the same secret as the established pseudonym)

Figure 13: Obtaining the Course Credential

9.4 Participating in the Evaluation

Here we present the API mapping for the use case GR9. This use case describes the steps needed for a student to be able to evaluate anonymously for a course. For more details about this use case please refer to Section 2.2.9 in [ADFS12]).

Table 5. Participating in the Course Evaluation

Step	Explanation

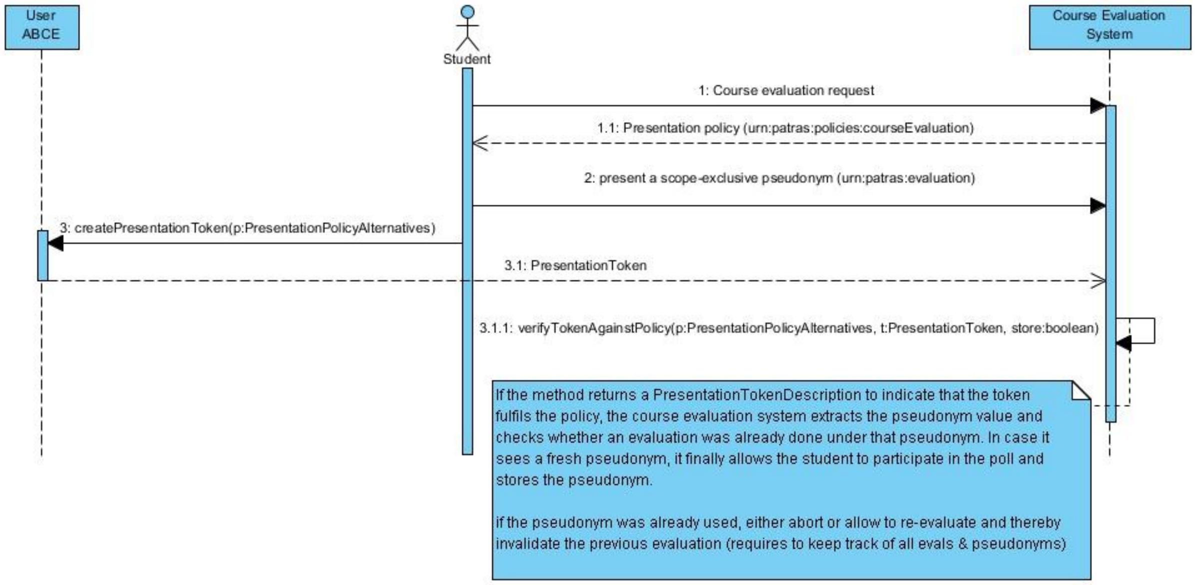
1	The student wants to evaluate a course.
	The course evaluation system sends the presentation policy *urn:patras:policies:courseEvaluation* for the associated credCourse:
	`<abc:PresentationPolicyAlternatives`
	`  xmlns:abc="http://abc4trust.eu/wp2/abcschemav1.0"`
	`  Version="1.0">`
	`  <abc:PresentationPolicy PolicyUID="urn:patras:policies:courseEvaluation">`
	`     <abc:Message>`

```
        <abc:Nonce>bkQydHBQWDR4TUZzbXJKYUphdVM=</abc:Nonce>
     </abc:Message>
     <abc:Pseudonym Exclusive="true" Scope="urn:patras:evaluation"
nym="#nym"/>
     <abc:Credential Alias="#credCourse" SameKeyBindingAs="#nym">
       <abc:CredentialSpecAlternatives>

<abc:CredentialSpecUID>urn:patras:credspec:credCourse</abc:CredentialSpecUID>
       </abc:CredentialSpecAlternatives>
       <abc:IssuerAlternatives>

<abc:IssuerParametersUID>urn:patras:issuer:credCourse</abc:IssuerParametersUI
D>
       </abc:IssuerAlternatives>
    </abc:Credential>
  </abc:PresentationPolicy>
</abc:PresentationPolicyAlternatives>
```

2	The student presents a scope-exclusive pseudonym for the scope *urn:patras:evaluation*, to ensure that each student can create only a single pseudonym for this purpose.
3	The student invokes the *createPresentationToken(p:PresentationPolicyAlternatives)* method with the received presentation policy to obtain the presentation token containing the requested information. When the smart recognizes that it should participate in the generation of a presentation token related to the credCourse, it checks if the counter value of the associated counter blob exceeds the threshold that is contained in the counter blob as well. Only if this check succeeds, the smart card will proceed with the generation of its part of the presentation token, and indicate failure otherwise.
4	The course evaluation system calls the ABCE method *verifyTokenAgainstPolicy(p:PresentationPolicyAlternatives, t:PresentationToken, store:boolean)* on the token and the policy. If the method returns a *PresentationTokenDescription* to indicate that the token fulfils the policy, the course evaluation system extracts the pseudonym value and checks whether an evaluation was already done under that pseudonym.


User ABCE
Student
Course Evaluation System
1: Course evaluation request
1.1: Presentation policy (urn:patras:policies:courseEvaluation)
2: present a scope-exclusive pseudonym (urn:patras:evaluation)
3: createPresentationToken(p:PresentationPolicyAlternatives)
3.1: PresentationToken
3.1.1: verifyTokenAgainstPolicy(p:PresentationPolicyAlternatives, t:PresentationToken, store:boolean)

If the method returns a PresentationTokenDescription to indicate that the token fulfils the policy, the course evaluation system extracts the pseudonym value and checks whether an evaluation was already done under that pseudonym. In case it sees a fresh pseudonym, it finally allows the student to participate in the poll and stores the pseudonym.

if the pseudonym was already used, either abort or allow to re-evaluate and thereby invalidate the previous evaluation (requires to keep track of all evals & pseudonyms)

Figure 14: Course Evaluation

10 Network Set up and Operation

The Patras Portal, the University Registration System, the Course Evaluation System and the Revocation Authority will be placed on DMZ and they will have their own IP addresses. Figure 15 presents Patras Pilot network infrastructure. The Course Evaluation System and Revocation Authority are equipped with their own servers and database repositories. The University Registration System is equipped with the Privacy-ABC server, the IdM server and its repository. DMZ includes both Patras Portal and the IdM public directory. All incoming HTTP/HTTPS requests go through DMZ.

The network security is ensured by the existence of a pair of firewalls (Cisco Pix-535) connected for high availability configuration (active-standby, and without NAT). Firewalls are connected between the border router (Cisco 7300 series) and the CTI internal network, inspecting incoming and outgoing traffic, ensuring network security and protection against malicious attacks. Firewalls can block source IP addresses in the case of DoS attacks and traffic to non-authorized addresses in CTI's internal network but cannot block packets with malicious content. We have also implemented a DMZ subnet. In the DMZ we have all the servers (e.g. web and VPN servers) that offer public services and they don't have any connection to the internal network of CTI. The VPN servers support the VPN connections that are necessary for the administration of Patras Pilot.

Moreover the University Registration System and Course Evaluation System will have their own, static, non-shared IP addresses which are reachable via the Internet. Also at the edge of our network there is a border router deployed in front of CTI's firewalls and performs some basic checks on network activity, such as ingress and egress filtering[1], that may be helpful for stopping some Internet-based worms from reaching the CTI's firewall. In border router we have implemented some generic access lists in order to increase the level of security and confront some types of malicious attacks like DoS or DDoS. Additionally in the two internal routers we have access lists, and through them we are able to specify which users or system processes are granted to access objects, as well as what operations are allowed on given objects, where objects are network devices, servers and workstations.

In order to protect HTTP/HTTPS incoming traffic we will implement access lists and rules according risk management requirements of Patra's Pilot (see Chapter 1). In order to have different roles of users, University Registration System and Course Evaluation System will be employed with different user accounts. The students will have local user accounts on the University Registration System. Administrators will use Active Directory in order to have access to the Course Evaluation System or the University Registration System via CTI's internal network or the Internet. Moreover lectors will have local user accounts on the Course Evaluation System for uploading their course questionnaire.

When a user make an HTTP request via internet, his HTTP connection will be routed from GRNet router to CTI's border router, and then after passing the firewalls and the internal routers the user will access the University Registration System or the Course evaluation Application in the DMZ by using the ABC technology. Administrators of the Patras Pilot can access the DMZ via Https/HTTP/SSH/LDAP connections through CTI's internal network or the Internet via a VPN connection. Administrators will follow the above traffic path like users in order to establish an HTTPS/HTTP connection. When an administrator wants to establish SSH/LDAP connection via the Internet, he must establish a VPN connection though a secure channel in order to get access the CTI's internal network and get a virtual IP at CTI's internal network [TN1029].

The Domain Controller server verifies the administrator's credentials and AAA server[2] authenticates him and allows him to get access to CTI's internal network. Once the administrator can connect to CTI's internal network he can access to the University Registration and Course Evaluation in DMZ.

[1] Ingress and egress filtering is done for intrusion detection, by establishing the origin of the communication.

[2] Authentication Authorisation Access Server; a common element in Mobile Networks

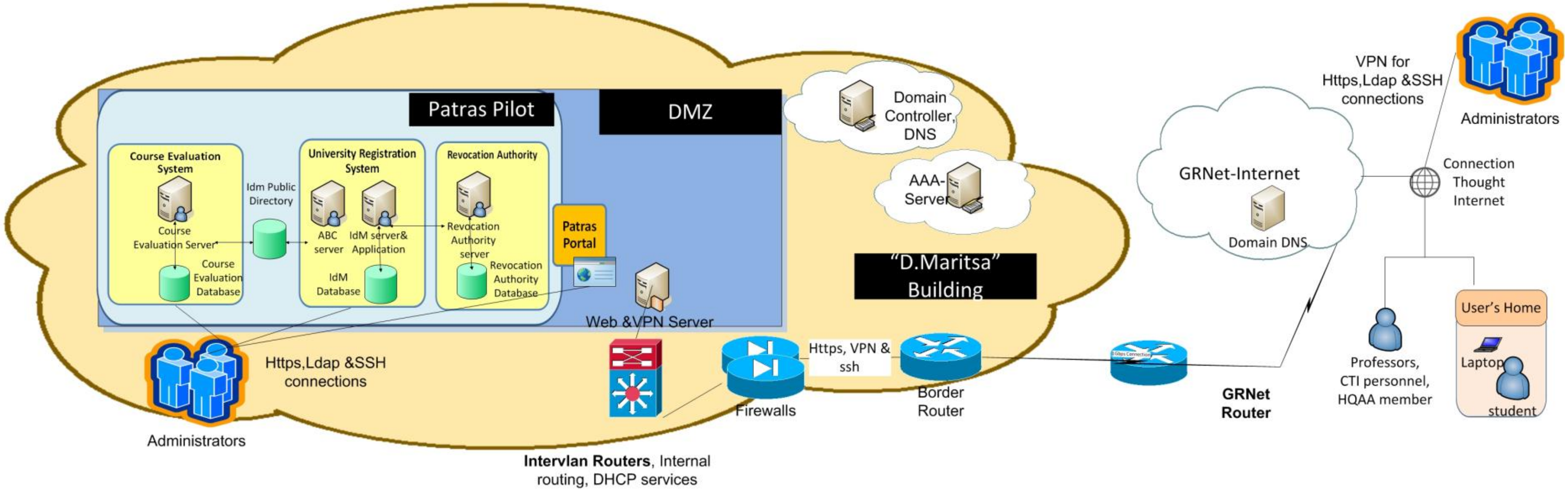


Figure 15: Patras Pilot network overview

11 Risk Management

In this section we present and discuss the results of applying a novel security- and privacy-aware Quantitative Threat Modeling Methodology (QTMM [QTMM12]) to the *ABC-related stages*[c] of the Patras pilot, with the goals of *(i)* identifying the potential risks and, *(ii)* eliciting the adequate set of security and privacy requirements. The results presented in this chapter only contain those identified threats that could not be further mitigated in the current version of the deployed system, but that nevertheless might have a noticeable risk/impact. These results might be used to further improve the security and privacy levels of the Patras pilot in the following iteration.

In order to keep homogeneity with the rest of this deliverable, the present chapter is organized according to the use cases identified for this pilot namely, Setup (Section 11.2), Registration & Login of Students (Section 11.3), Obtaining University and Course Credentials (Section 11.4), Certification of Class Attendance (Section 11.5), Participation in Evaluation (Section 11.6) and, Backup & Restore (Section 11.7). Before presenting the actual results of the QTMM, the next section overviews the basic concepts of this methodology.

11.1 Overview of the applied Quantitative Threat Modeling Methodology

While the general concept of "Privacy-by-Design (PbD)" is increasingly a popular one, there is considerable paucity of either rigorous or quantitative underpinnings supporting PbD. Drawing upon privacy-aware modeling techniques, this section overviews the basic concepts of a novel Quantitative Threat Modeling Methodology (QTMM) that has been proposed in the context of ABC4Trust. The QTMM was applied to the Patras pilot to draw objective conclusions about the different privacy and security related attacks that might affect it. Interested readers are referred to [QTMM12] for further details about the QTMM.

The QTMM comprises the five steps shown in Figure 16, where an informal use case description is the entry point to elicit a set of optimal security and privacy requirements. The rest of this section presents, with the level of detail required by this document, each one of the QTMM's steps.

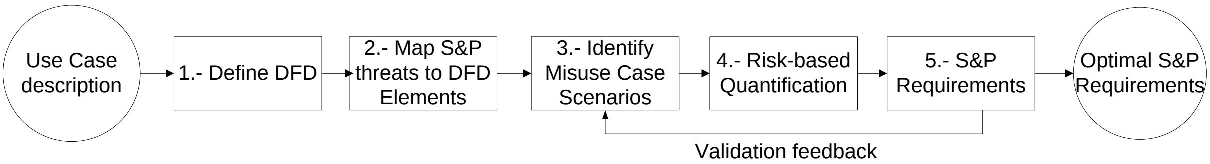

Use Case description
1.- Define DFD
2.- Map S&P threats to DFD Elements
3.- Identify Misuse Case Scenarios
4.- Risk-based Quantification
5.- S&P Requirements
Optimal S&P Requirements
Validation feedback

Figure 16: Overview of the applied QTMM

[c] I.e., Setup, Registration and Login, Obtaining University and Course credentials and, Participating in the evaluation.

11.1.1 Step 1: Define Data Flow Diagrams (DFD)

In general, DFDs [DFD93] can aid the formal decomposition of a system such that the elements of Entities, Trust Boundaries, Data Flows, Data Sources and Processes are clearly identified. A DFD is a graphical representation of data flows, data stores, and relationships between data sources and destinations (entry and exit points). The guiding principle for DFDs is that an application or a system can be decomposed into subsystems, and subsystems can be decomposed into recursive lower-level subsystems. This iterative process makes DFDs useful for decomposing applications to analyze the associated threats at varied levels of detail. Typically, in a DFD only the abstract/high-level views of the interactions among the different components of a system are represented (mostly at the service-level), rather than the messages exchanged via the underlying protocol.

The DFD used for the threat analysis of the Patras pilot is shown in the following Figure 17. Please notice that the level of detail shown in this DFD corresponds to the performed analysis for example, *we have not analysed the S&P threats related with the internals of the ABCE subsystem*.

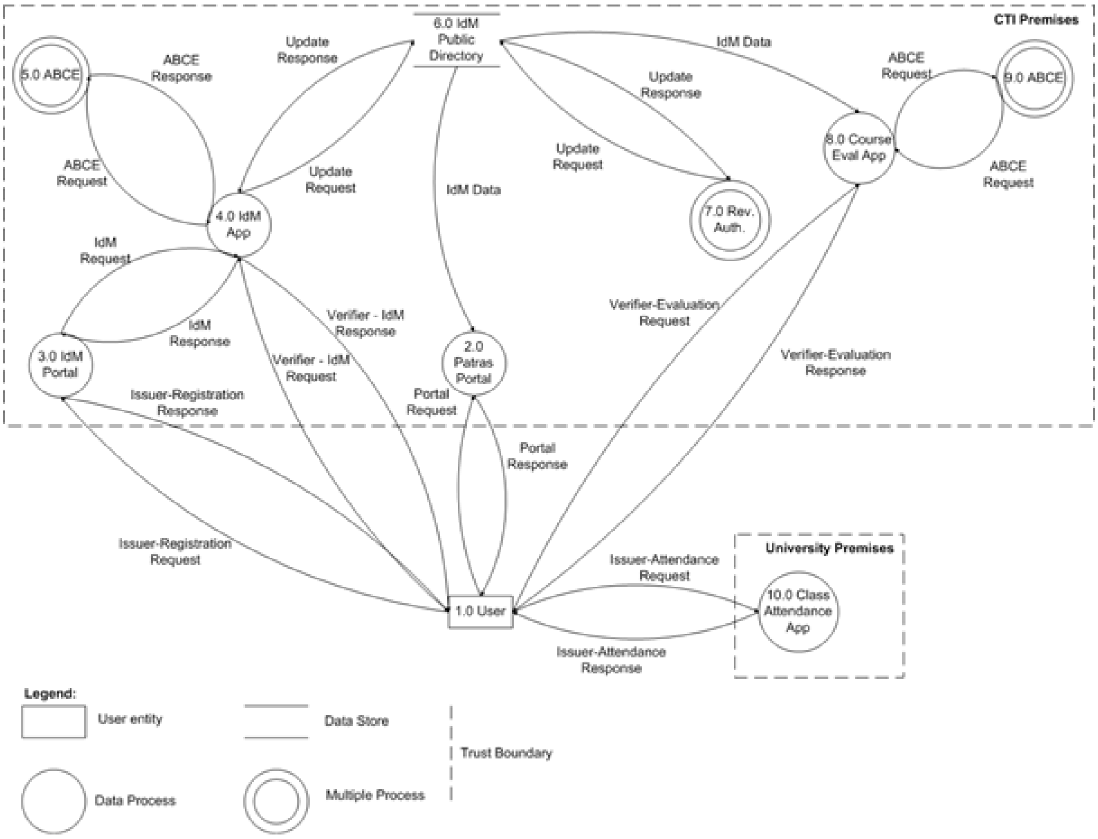


Figure 17: Data Flow Diagrams

11.1.2 Step 2: Map S&P threats to DFD elements

During this stage, the set of newly created DFDs are "mapped" to the threats associated with each one of the security and privacy properties to be taken into account for the QTMM. The specific properties taken into account comprise the "traditional" security ones (i.e., Confidentiality, Integrity and Availability) plus the ones proposed in [PPG12] for privacy (i.e., Unlinkability, Transparency and Intervenability). In the applied QTMM, the set of S&P threats being considered (along with their corresponding DFD mapping is shown in Table 4). The rationale behind the proposed mapping can be found in [QTMM12].

Table 4. Mapping S&P properties to DFD elements (DF= Data Flow. DS= Data Source, P= Process, E= Entity)

S&P property	S&P threat	Threat explanation	DF	DS	P	E
Confidentiality	Information Disclosure	These threats expose personal information to individuals who are not supposed to have access to it.	X	X	X	
Integrity	Tampering	Tampering is the unauthorized modification of data, for example as it flows over a network between two computers	X	X	X	
Availability	Denial of Service	Denial of service is the process of making a system or application unavailable.	X	X	X	
Unlinkability	Linkability	For two or more items of interest (IOIs, e.g., subjects, messages, actions, etc.) allows an attacker to sufficiently distinguish whether these IOIs are related or not within the system.	X	X	X	X
Transparency	Unawareness	Indicates that one or more parties are unaware of the conditions related with privacy-relevant data processing.				X
Intervenability	Avoidance/Non-intervenability	Indicates that the parties related with the privacy-relevant data processing, are unable to interviene.			X	X

For the Patras analysis, the S&P to DFD mapping is shown in Table 5. From this table it is worth to highlight the following assumptions about each one of the threats under analysis:

- No threats were analyzed wrt. ABCE-specific components (including Data Flows and Processes). This analysis is taking part in WP2 and WP3.

- Disclosure threats do not apply to the “IdM Public Directory” and, only applies to Data Flow containing personal data.
- Denial of Service threats are *system-wide* and, can compromise any of the DFD elements (in particular Data Stores and Processes).

Table 5. Mapping S&P threats to the Patras' DFD

		S&P threats[d]					
DFD component	**Threat Target**	**I**	**T**	**D**	**L**	**U**	**A**
Data Store							
	IdM Public Directory (6.0)	X	6	0*	X		
Data Flow							
	Class Attendance System - User (1.0 – 10.0)	1	X	X	12		
	Course Evaluation System – ABC System (8.0 - 9.0)	X	X	X	X		
	Course Evaluation System – User (1.0 - 8.0)	2	7	X	13		
	IdM App - IdM Portal (3.0 - 4.0)	X	X	X	X		
	IdM App – ABC System (10.0 - 11.0)	X	X	X	X		
	IdM App – User (4.0 - 5.0)	X	X	X	X		
	IdM Portal – User (1.0 – 3.0)	3	8	X	X		
	Patras Portal - User (1.0 - 2.0)	X	X	X	X		
	Public Directory – Course Evaluation System (8.0 – 6.0)	X	X	X	X		
	Public Directory – IdM App (4.0 - 6.0)	X	X	X	X		
	Public Directory – Patras Portal (2.0 - 6.0)	X	X	X	X		
Process							
	Class Attendance Application (10.0)	X	X	0*	X		x
	Course Evaluation System (8.0)	4	9	0*	14		X
	IdM Application (4.0)	X	X	0*	X		16
	IdM Portal (3.0)	5	10	0*	X		x

[d] Table 4 includes threats description.

	Patras Portal (2.0)	X	11	0*	X		x
Entity							
	User (1.0)				X	15	17

11.1.3 Step 3: Identify Misuse Case Scenarios

It is a common practice in threat modelling to document a threat analysis as “misuse case scenarios”, where details are specified about generic threats that can be posed as specific threat instances in a real system. Misuse cases can be documented in different ways, but in general the analysis should provide information about the attacker model, a summary of the attack, a set of assumptions/preconditions to launch the attack and the relevant attack tree [AT99]. Our QTMM uses attack trees in order to quantify threats and prioritize the elicitation of S&P mechanisms (this will be shown in the next section).

For the Patras’ pilot *our first analysis identified a total of 17 misuse cases*, corresponding to the mapping shown in Table 5. The attacker model we assume for all the misuse cases are *skilled insiders or skilled outsiders* (i.e., are able to read/write data from/to DFD elements) *with a finite amount of resources* (e.g., they will not be able to break the underlying cryptography in a finite period of time). Furthermore, the first iteration of the QTMM considers that *no S&P mechanisms have been implemented*. For example, Data Flows are unencrypted, no Privacy-ABC technology is integrated into the pilot, etc. Thanks to this basic assumption, it is possible to perform an iterative elicitation process, just as described in the next section. The final set of misuse cases (after eliciting the final S&P requirements) will be summarized in Sections 11.2- 11.7.

11.1.4 Step 4: Risk-based Quantification

The essence of our proposed QTMM is an approach to quantify the S&P risks associated with each element of an attack tree (threats and attacks). Our methodology contributes with the techniques to provide an overall quantitative score for the whole threat based on its individual attacks. This score can be used by designers and decision makers to e.g., prioritize the identified threats and begin the elicitation of the required mitigation mechanisms. Using a “score card” approach, the QTMM proposes to quantify two basic parameters on the attack trees:

- Impact: the damage potential (including affected users) of the threat/attack. Score card: (1) Insignificant,(2) Minor, (3) Moderate, (4) Major, and (5) Catastrophic.
- Risk: the likelihood of a threat/attack. Score card*: (1) Rare, (2) Unlikely, (3) Possible, (4) Likely, and (5) Certain.*

Due to space limitations, we will not explain in further details how to actually aggregate the former two parameters on the attack trees. However, interested readers are referred to [QTMM12] for more details.

11.1.5 Step 5: S&P Requirements

The final stage in traditional threat analyses is the elicitation of specific mitigation techniques. By the contrary, our QTMM approach is in fact an iterative process where elicited S&P requirements (mitigation techniques) are used to refine both the misuse cases and corresponding attack trees (quantified impacts and risks) during each iteration. This refinement process finalizes until a set of S&P requirements/mechanisms allows managing risks optimally (i.e., either to avoid, optimize or accept the resulting risk).

The rest of this chapter presents the final results (*only the final residual/accepted risks*) after iterating two times the QTMM in the Patras' pilot.

11.2 Setup

During the Setup stage of the Patras pilot, the threats that continue having the highest impact/risk are those related with the tamper of either the setup parameters, the ABCE API or the Credential Specification (cf.Table 6).

Table 6. QTMM results: Setup

Threat Name	**Threat Class***	**Comments**	**Impact****	**Risk*****	**Proposed mitigation**
Unauthorized modification of Credential Specification.	T	The attacker is able to modify the Credential Specification stored in the IdM Public Directory.	4	3	Protect the integrity/authenticity of the Credential Specification e.g., via hashes or digital signatures+.
Unauthorized modification of Issuer parameters	T	The attacker can modify the Issuer's initialization parameters.	5	3	University Registration System signs the produced Issuer Parameters. The SC verifies the integrity/authenticity of initialization parameters ·
Unauthorized modification of the ABCE API.	T	The attacker can distribute a malicious/customized copy of the ABCE API.	5	2	Protect the integrity/authenticity of the ABCE API binary via e.g., hashes or digital signatures+.

** (I)nformation Disclosure, (T)ampering, (D)enial of Service, (L)inkability, (U)nawareness, (A)voidance*

*** (1) Insignificant, (2) Minor, (3) Moderate, (4) Major, (5) Catastrophic*

**** (1) Rare, (2) Unlikely, (3) Possible, (4) Likely, (5) Certain*

+ To be addressed in the next version of the trial.

11.3 Registration & Login of Students

For both of these processes, information disclosure attacks are possible to launch if there are no minimum security countermeasures implemented at the University Registration System (e.g., firewalls, intruder detectors, etc.). Table 7 shows in further detail the results of our threat analysis (only threats with accepted/non-mitigated risks are shown).

Table 7. QTMM results: Registration and Login

Threat Name	**Threat Class***	**Comments**	**Impact****	**Risk*****	**Proposed mitigation**
Denial of Service (DoS) against the University Registration System.	D	The attacker performs a DoS attack against the University Registration System.	3	1	The University Registration system's security is ensured by the existence of a pair of firewalls, inspecting incoming and outgoing traffic, ensuring network security and protection against malicious attacks. More details about systems and network security will be described in Network set up and operation section (cf., Section 10).
Information Disclosure by impersonating the Student via the login Presentation Token.	I	The attacker is able to disclose the student's information contained in the. University Registration System's database, by	4	1	The login Presentation Token uses a nonce (embedded into the corresponding Presentation Policy). The DMZ that hosts these

		impersonating her via login Presentation Token (replay attack).			systems is equipped with an underlying anonymous communication protocol.
Information Disclosure on University Registration System's data flow.	I	The attacker obtains student's personal data by capturing the traffic between the student and the University Registration System.	4	1	The DMZ that hosts these systems uses a secure and authenticated communication channel (e.g. SSL/TLS, WS-Security) for its communications.
Information Disclosure on University Registration System's Presentation Policy.	I	The attacker can modify the Presentation Policy used by the University Registration System for the registration stage, in order to disclose an unauthorized set of student's attributes.	4	3	Due diligence[e] related with the security of the University Registration System. Protect the integrity/authenticity of the Presentation Policy via e.g., hashes or digital signatures[+].
Information Disclosure on University Registration System's student database.	I	The attacker compromises the University Registration System's student database/logs to access the personal data stored there.	4	2	The University Registration system's security is ensured by the existence of a pair of firewalls, inspecting incoming and outgoing traffic, ensuring network security and protection against malicious attacks. More details about systems and network security will be described in Network set up and operation section (cf., Section 10).

** (I)nformation Disclosure, (T)ampering, (D)enial of Service, (L)inkability, (U)nawareness, (A)voidance*

*** (1) Insignificant, (2) Minor, (3) Moderate, (4) Major, (5) Catastrophic*

**** (1) Rare, (2) Unlikely, (3) Possible, (4) Likely, (5) Certain*

[+] *To be addressed in the next version of the trial.*

[e] Best effort measures.

11.4 Obtaining University and Course Credentials

The set of accepted threats related with these issuance processes are similar to the ones shown in Table 7, with exception of a new impersonation threat that might appear if the bound pseudonym-smartcard is not verified.

Table 8. QTMM results: Obtaining University and Course Credentials

Threat Name	Threat Class*	Comments	Impact**	Risk***	Proposed mitigation
Denial of Service (DoS) against the University Registration System.	D	The attacker performs a DoS attack against the University Registration System.	3	1	The firewalls protecting the University Registration System can block both source IP addresses (in the case of DoS attacks) and incoming traffic from non-authorized addresses in CTI's internal network.
Information Disclosure due to compromised smartcard.	I	A compromised smartcard/PIN might result in attacker disclosing the personal data of the correspondent student.	4	2	Due diligence of the student wrt. her smartcard. Use of Privacy-ABC's revocation feature+.
Information Disclosure of former student's personal data.	I	The attacker compromises historic logs files/databases of the University Registration System, to obtain personal data of former students.	3	2	Implement short retention periods of personal data related with revoked credentials.
Information Disclosure on University Registration System's data flow.	I	The attacker obtains student's personal data by capturing the traffic between the student and the University Registration System (issuance protocol).	4	1	The DMZ that hosts these systems uses a secure and authenticated communication channel (e.g. SSL/TLS, WS-Security) for its communications.

Information Disclosure on University Registration System's Issuance Policy.	I	The attacker can modify the Issuance Policy used by the University Registration System (for both *credUniv* and *credCourse*), in order to disclose an unauthorized set of student's attributes.	4	2	The University Registration system's security is ensured by the existence of a pair of firewalls, inspecting incoming and outgoing traffic, ensuring network security and protection against malicious attacks. More details about systems and network security will be described in Network set up and operation section (cf., Section 10). Protect the integrity/authenticity of the Issuance Policy via e.g., hashes or digital signatures[+].
Information Disclosure on University Registration System's student database.	I	The attacker compromises the University Registration System's student database/logs to access the personal data stored there.	4	1	The University Registration system's security is ensured by the existence of a pair of firewalls, inspecting incoming and outgoing traffic, ensuring network security and protection against malicious attacks. More details about systems and network security will be described in Network set up and operation section (cf., Section 10).

** (I)nformation Disclosure, (T)ampering, (D)enial of Service, (L)inkability, (U)nawareness, (A)voidance*

*** (1) Insignificant, (2) Minor, (3) Moderate, (4) Major, (5) Catastrophic*

**** (1) Rare, (2) Unlikely, (3) Possible, (4) Likely, (5) Certain*

[+] *To be addressed in the next version of the trial.*

11.5 Certification of Class Attendance

This stage has been temporarily implemented as a non-ABC solution, therefore was not considered in the threat modeling.

11.6 Participation in Evaluation

Most of the threats related with this stage, refer to tampering (illegally modifying) the evaluation results. The details are shown in Table 9.

Table 9. QTMM results: Participation in Evaluation

Threat Name	Threat Class*	Comments	Impact**	Risk***	Proposed mitigation
Denial of Service (DoS) against the Evaluation System.	D	The attacker performs a DoS attack against the Evaluation System.	3	1	The firewalls protecting the Evaluation System can block both source IP addresses (in the case of DoS attacks) and incoming traffic from non-authorized addresses in CTI's internal network.
Information Disclosure on Evaluation System's Presentation Policy.	I	The attacker can modify the Presentation Policy used by the Evaluation System, in order to disclose an unauthorized set of student's attributes.	4	2	The University Registration system's security is ensured by the existence of a pair of firewalls, inspecting incoming and outgoing traffic, ensuring network security and protection against malicious attacks. More details about systems and network security will be described in Network set up and operation section (cf., Section 10). Protect the integrity/authenticity of the Presentation Policy

					via e.g., hashes or digital signatures.
Tampering with the evaluation's results by allowing access to a non-valid student.	T	The attacker uses a set of non-valid credentials (e.g., a student that quit the course before the semester's finalization) to evaluate a course.	3	3	Implement Privacy-ABCs revocation feature^{+}.

* *(I)nformation Disclosure, (T)ampering, (D)enial of Service, (L)inkability, (U)nawareness, (A)voidance*

** *(1) Insignificant, (2) Minor, (3) Moderate, (4) Major, (5) Catastrophic*

*** *(1) Rare, (2) Unlikely, (3) Possible, (4) Likely, (5) Certain*

$^{+}$ *To be addressed in the next version of the trial.*

11.7 Backup & Restore

This process implements a customized mechanism for the non-ABC attendance temporal solution, therefore was not considered in the analysis.

12 Bibliography

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

[DSDBP12] S. Bcheri, N. Götze, V. Liagkou, A. Pyrgelis, C. Raptopoulos, Y. Stamatiou, K. Storf, P. Wängmark, Harald Zwingelberg. D5.1 Scenario definition for both pilots, 2012, https://abc4trust.eu/index.php/pub/

[DFD93] P. Bruza and T. van der Weide , "The semantics of data flow diagrams," in Proc. of the International Conference on Management of Data. McGraw-Hill, 1993, pp. 66-78.

[DSTICICC09] Directorate for Science, Technology and Industry Committee for Information, Computer and Communications. *POLICY, THE ROLE OF DIGITAL IDENTITY MANAGEMENT IN THE INTERNET ECONOMY: A PRIMER FOR POLICY MAKERS, 2009 http://www.oecd.org/dataoecd/55/48/43091476.pdf*

[Jetty] Jetty Web Server http://jetty.codehaus.org/jetty/

[Drupal] Drupal http://drupal.org/

[IRI2012] H. Guldage and J. Dam Nielsen, D4.1 Initial Reference Implementation, Version1, 2012.

[Mono] Mono Project http://mono-project.com/Main_Page

[AT99] B. Schneier , "Attack trees," Dr Dobb's, vol. 24, no. 12, 1999. [Online]. Available: http://www.schneier.com/paper-attacktrees-ddj-ft.html

[MySQL] MySQL: The world's most popular open source database http://www.mysql.com

[GNU GPL] GNU General Public License http://www.gnu.org/copyleft/gpl.html

[Drupal] Drupal http://drupal.org/

[PPG12] H. Zwingelberg and M. Hansen, "Privacy Protection Goals and their implications for eID systems," in Proc. of the IFIP International Summer School, 2011.

Appendix A User Manual

User Manual

Disclaimer*: The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.*

A.1 Introduction

A.1.1 Purpose

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.

As part of the ABC4Trust project that is supported by the ICT Programme of the European Union students and professors of the Computer Engineering and Informatics Department are being asked to participate in an online Course Evaluation system. More specifically, the system scope will be the realization of a trial 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.

The Computer Engineering and Informatics Department has the opportunity to introduce to the utilizing students and professors via the Course Evaluation System the Anonymous Based Credentials (ABC) technologies and to enable their efficient/effective deployment in practice.

This manual will give students, professors and othis education officials all the information they need to incorporate the Privacy-ABCs for online course evaluation in the Computer Science department of the University of Patras.

The manual addresses the following key content areas:

1. A generic information about ABC technologies and the ABC4Trust Project (see Subsections A.1.3 and A.1.4)
2. Description of Anonymous Course evaluation for certified students (see Section A.2)
3. A step-by-step description of how the course evaluation system operate and interact with its users (see Section A.3.8)

A.1.2 Overview

More precisely, in Section A.2 we give a description of Course Evaluation System for certified students. The University Pilot will take place in the Computer Engineering and Informatics Department of the University of Patras in Greece (see Figure 18). 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.

Figure 18: The Computer Engineering and Informatics Department

CTI will be responsible for formatting the group of students that will participate in the University pilot. The major challenge for University Pilot 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, the participated students will have to do the following steps in order to evaluate the two selected courses in a way that ensures the credibility of results and preserves the privacy of the students expressing their opinion:

1. All the participated students will have in their possession a smart card (see Section A.3.1).
2. They have to register their smart card. (see Section A.3.2)
3. Then any student can be registered at the Computer Engineering and Informatics Department University or pick a course by using the ABC technology (see Section A.3.3).
4. All the students that will take part in the evaluation can collect their attendance information at each lecture (see Section A.3.5).
5. Each student can back up his attendance information and to restore backed up data on his (new) smart card (see Section A.3.6).
6. They will prove that they are indeed students of the department offering the course, they are registered to the course under evaluation and they have attended sufficient number of lectures. In order to submit their course evaluation (see Section A.3.8).

A.1.3 Attribute-based Credentials

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.

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.

A.1.4 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. 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 in two specific environments.

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 [Fumy11]. 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.

A.2 University Pilot Description

A.2.1 Before the Semester

CTI will conduct two trials and an on-site testing of Course Rating 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 trials, CTI will select 3 to 5 student-volunteers in order to participate to an on-site testing of Course Rating by certified students. For the main trials 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.

A group of 25 students that will take part in the evaluation of two courses will obtain a smart card, a password and a PIN (see Section A.3.1).

A.2.2 During the Semester

Students of Computer Engineering and Informatics Department will be issued credentials that certify a number of facts about them:

1. They are eligible students of the at the Computer Engineering and Informatics Department University
2. They have picked a course (see Section A.3.4).

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. All the participated students 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 your own data using these credentials.

Moreover each student can collect his attendance information by waving his smart cart in front of a contactless NFC reader when leaving the lecturing room. Student's smart-card is updated every time he attends a class (see Section A.3.5). Each student can back up his attendance information and to restore backed up data on his (new) smart card at any time he wants. 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 you visited. This scenario uses the Class Attendance system presented in pilot's architecture in order to collect students' attendance information.

A.2.3 At the End of Semester

There will be two rounds of 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 June 2013. This will assure that the second trial 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 trial.

This Course Evaluation scenario 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.

The participated students will be able to anonymously rate courses that 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.

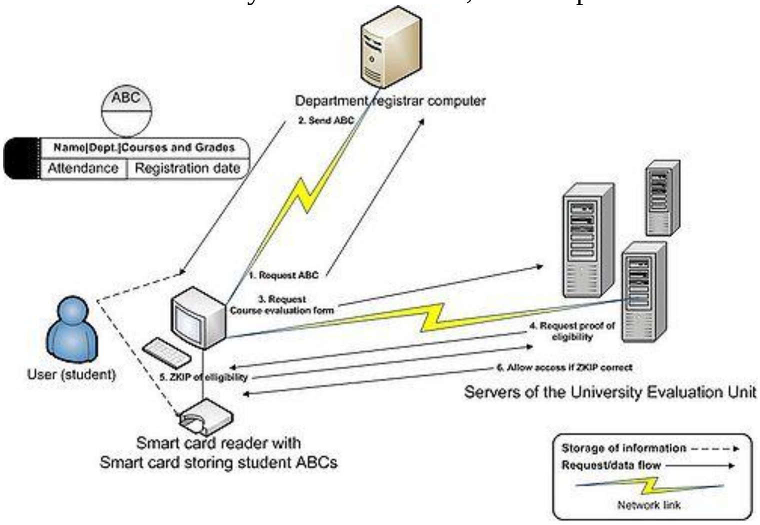
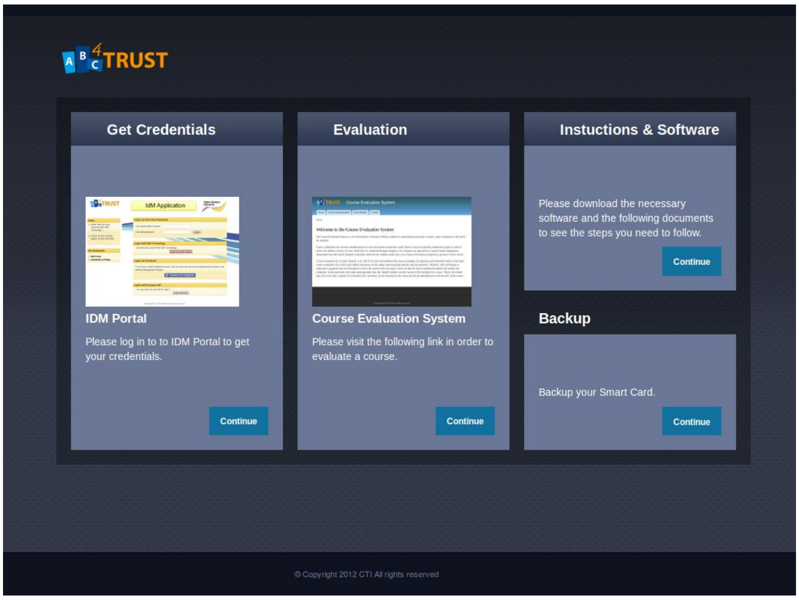

ABC
Name|Dept.|Courses and Grades
Attendance
Registration date
Department registrar computer
2. Send ABC
1. Request ABC
3. Request Course evaluation form
4. Request proof of eligibility
5. ZKIP of elligibility
6. Allow access if ZKIP correct
User (student)
Servers of the University Evaluation Unit
Smart card reader with Smart card storing student ABCs
Storage of information
Request/data flow
Network link

Figure 19: University Pilot Overview

A.2.4 University Pilot Portal

University Pilot Portal is an information web portal (see Figure 20). Through this portal, all the students 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, his first action is to visit this portal and by following the instructions he can perform various pilot operations (e.g. register to a course, evaluate a course).



Get Credentials

IDM Portal

Please log in to to IDM Portal to get your credentials.

Evaluation

Course Evaluation System

Please visit the following link in order to evaluate a course.

Instuctions & Software

Please download the necessary software and the following documents to see the steps you need to follow.

Backup

Backup your Smart Card.

© Copyright 2012 CTI All rights reserved

Figure 20: University Pilot's Portal

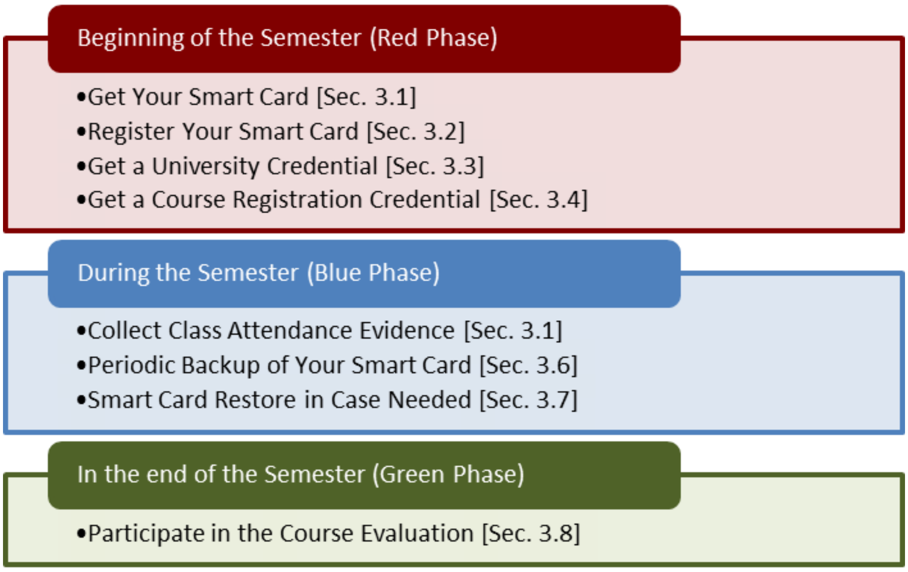
As the Figure 20 shows it consists of three blocks: Get Credentials, Evaluation, Instructions & Software. Get Credentials and Evaluation blocks describe the University Registration System and Course Evaluation System respectively and with the button Continue the student visits their site. In the Instructions & Software block you can find a User Guide and the necessary software for the evaluation process.

- To Access Patras Portal Follow the link: https://ces.cti.gr/Portal/Portal.html

A.3 Participating in the Pilot

Welcome to the ABC4Trust pilot!

In this section we provide a step-by-step description of the actions you need to take in order to successfully participate in ABC4Trust pilot. A quick overview of all the activities is shown in Figure 21. As you see we have three phases (Red, Blue and Green) for a semester and each one requires you to follow certain steps in order to enable the next phase.



Beginning of the Semester (Red Phase)

- Get Your Smart Card [Sec. 3.1]
- Register Your Smart Card [Sec. 3.2]
- Get a University Credential [Sec. 3.3]
- Get a Course Registration Credential [Sec. 3.4]

During the Semester (Blue Phase)

- Collect Class Attendance Evidence [Sec. 3.1]
- Periodic Backup of Your Smart Card [Sec. 3.6]
- Smart Card Restore in Case Needed [Sec. 3.7]

In the end of the Semester (Green Phase)

- Participate in the Course Evaluation [Sec. 3.8]

Figure 21: A Quick Overview of pilot

As a summary of the whole process, you will receive a smart card package that enables you to interact with the system. After the necessary initializations that are described in the following sections you need to download certified credentials that can help you prove your registration in the university and enrollment in the course. At this point the Red Phase is over and you can begin with the Blue Phase. You need to use your smart card to collect the attendance data for each lecture of the pilot course that you participate. These evidences are necessary to prove that you are eligible for evaluating the course. Since your smart card is the only place that this information is stored, you must periodically make backups of the card data so that in case of loss or defeat, you can restore them into a new card. When you reach the end of the semester, the Green phase will start and you can follow the given steps to express your opinion about the course anonymously.

Note:

- ***You must have in your possession a smart card with a user secret, a PIN and a PUK.***
- ***You must have also a smart card reader.***

A.3.1 How to get your Smart Card

The department's Registration Office will provide you your smart card package after you signed the necessary documents and gave your consent to participate in the pilot. In particular, this package contains the following items:

☑ A smart card
☑ A smart card reader
☑ A sealed envelope that is marked with the smart card ID and contains your smart card's PIN and PUK.
☑ A slip of paper containing a one-time-password (OTP)

When you receive this package, the University Registration office records your name, envelope's identification number (=smart card IDs) and the corresponding OTP.

A.3.2 How to Register Your Smart Card

This phase describes the procedures required so that the students can register their smart cards.

How to Register Your Smart Card - Step 1:

Plug the USB cable of card Reader to your computer and place the smart card into the card Reader as the **Figure 22** shows. Otherwise, you can use the University's card readers, which are located in the computer center.

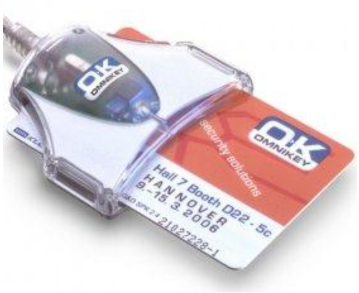
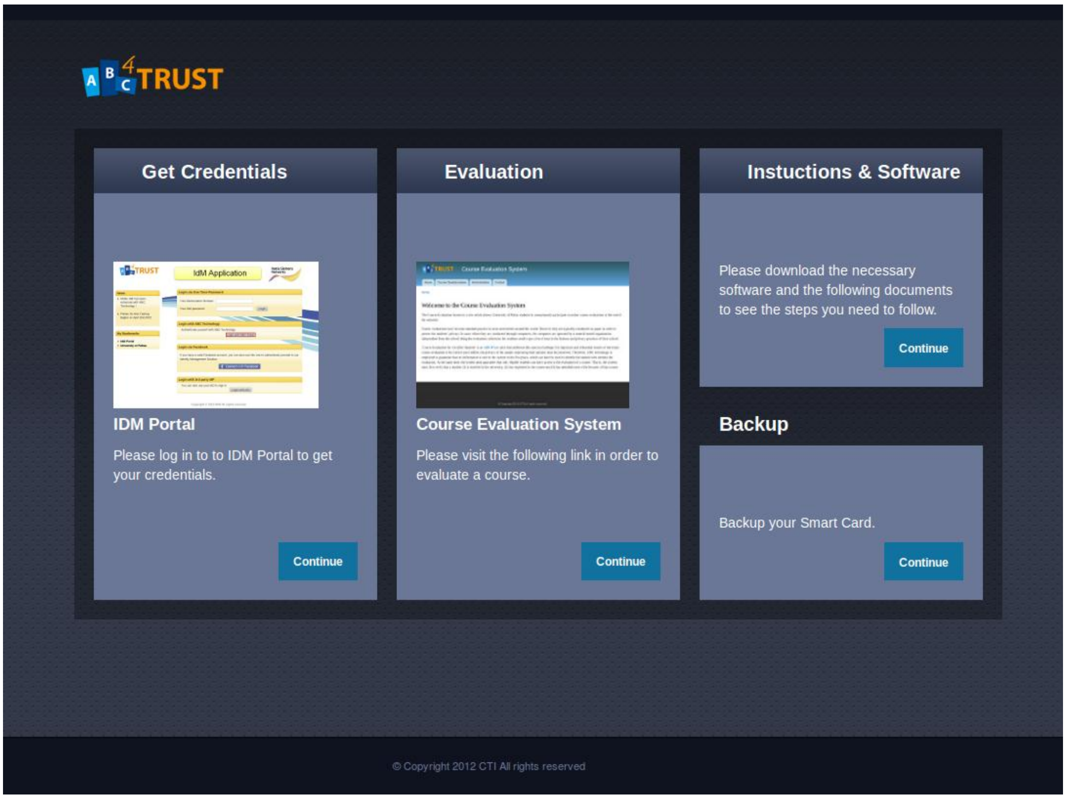


Figure 22: Smart card reader

How to Register Your Smart Card - Step 2:

Visit Patras Portal site at https://ces.cti.gr/Portal/Portal.html. You will see the following interface on your screen. Follow the link for “Get Credential”.



Get Credentials

IDM Portal

Please log in to to IDM Portal to get your credentials.

Evaluation

Course Evaluation System

Please visit the following link in order to evaluate a course.

Instuctions & Software

Please download the necessary software and the following documents to see the steps you need to follow.

Backup

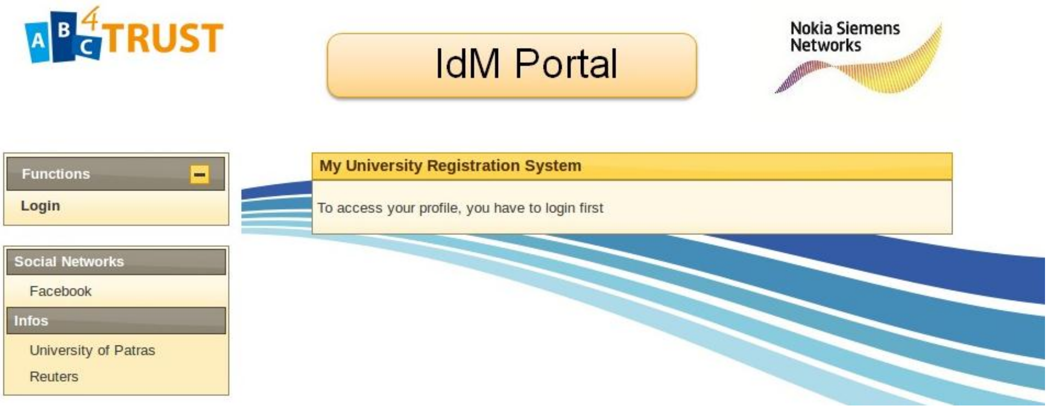
Backup your Smart Card.

© Copyright 2012 CTI All rights reserved

Figure 23: Patras Portal

How to Register Your Smart Card - Step 3:

Now you are redirected to IDM Portal welcome page as shown in the following **Figure 24**. Please click on the "Login" link on the left column of this page.

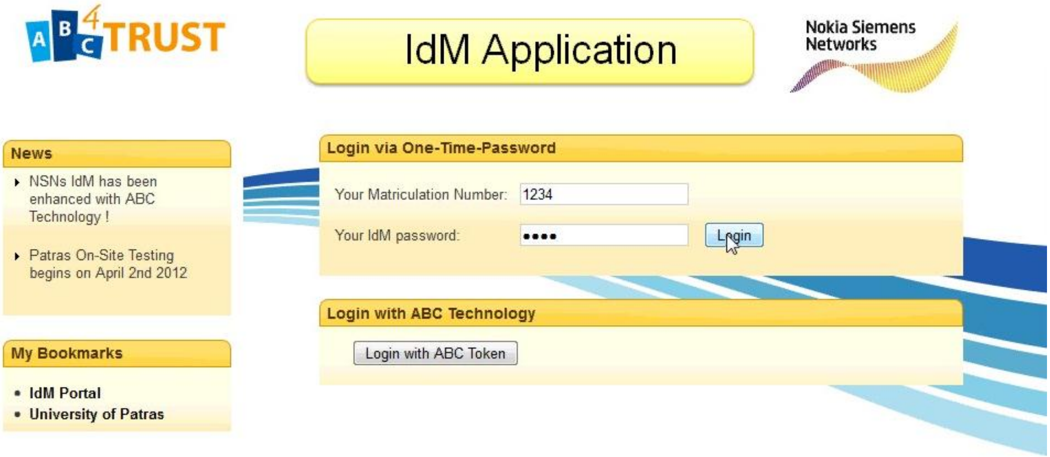


To access your profile, you have to login first

Figure 24: IdM Welcome Page

How to Register Your Smart Card - Step 4:

At this point you need to login via your One-Time-Password (OTP). Enter your matriculation number and your OTP in the corresponding box as shown the **Figure 25** below and click on the login button.


IdM Application

News
- NSNs IdM has been enhanced with ABC Technology !
- Patras On-Site Testing begins on April 2nd 2012

My Bookmarks
- IdM Portal
- University of Patras

Login via One-Time-Password

Your Matriculation Number: 1234

Your IdM password: ••••

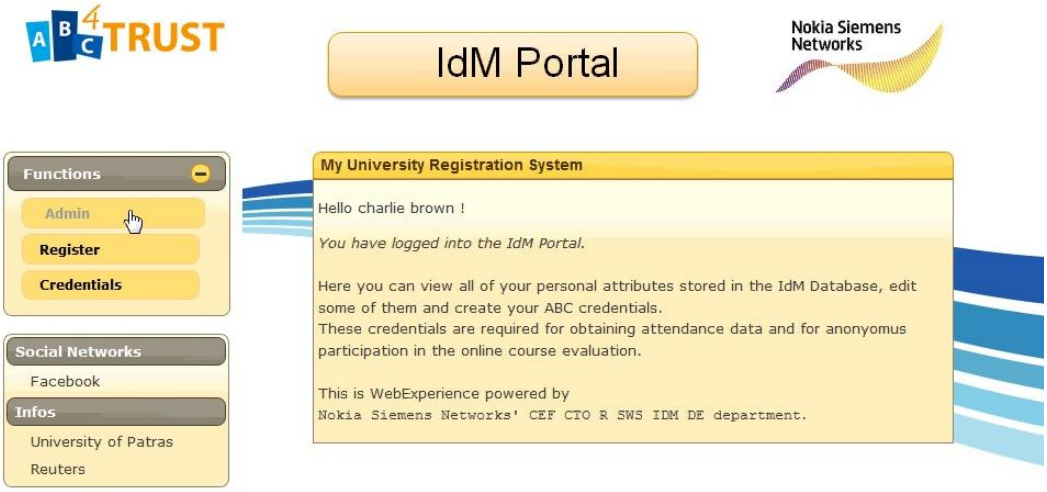
Login with ABC Technology

Figure 25: Login using Matriculation No and OTP

How to Register Your Smart Card - Step 5:

If the authentication is successful you will see a welcome message (**Figure 26**).

Now you can access your account information and all your attributes under the "Admin" menu (Figure 27). To continue with smart card registration click on "Register".



My University Registration System

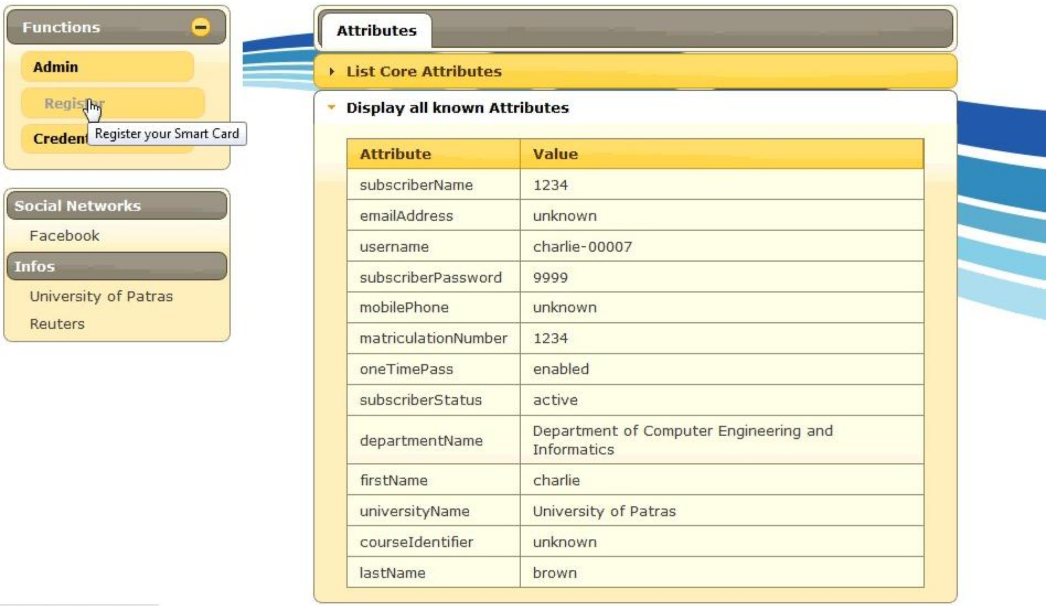
Hello charlie brown !

You have logged into the IdM Portal.

Here you can view all of your personal attributes stored in the IdM Database, edit some of them and create your ABC credentials.
These credentials are required for obtaining attendance data and for anonyomus participation in the online course evaluation.

This is WebExperience powered by
Nokia Siemens Networks' CEF CTO R SWS IDM DE department.

Figure 26: Login welcome message

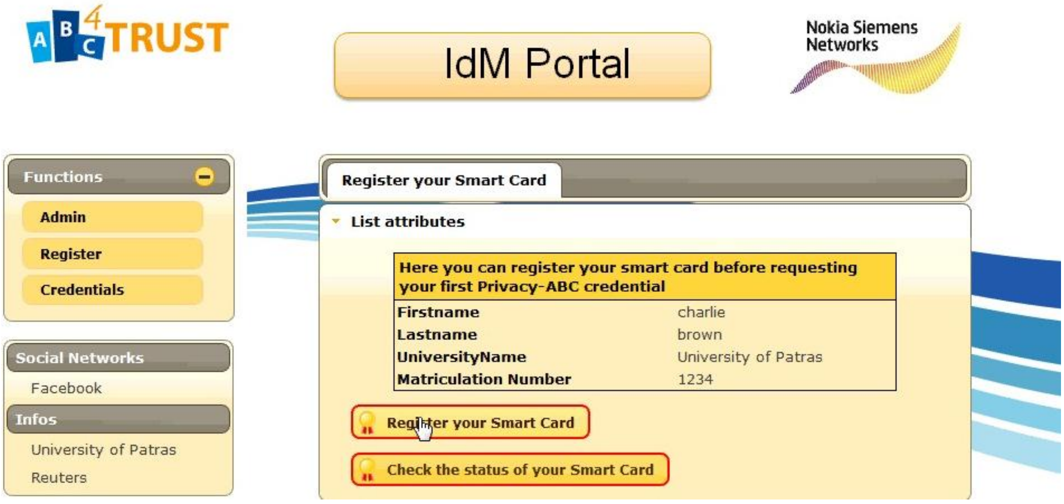


Attribute	Value
subscriberName	1234
emailAddress	unknown
username	charlie-00007
subscriberPassword	9999
mobilePhone	unknown
matriculationNumber	1234
oneTimePass	enabled
subscriberStatus	active
departmentName	Department of Computer Engineering and Informatics
firstName	charlie
universityName	University of Patras
courseIdentifier	unknown
lastName	brown

Figure 27: Attributes list

How to Register Your Smart Card - Step 6:

At this point you should be seeing the page shown in the figure below. Please click on the link “Register your Smart Card”.



Here you can register your smart card before requesting your first Privacy-ABC credential	
Firstname	charlie
Lastname	brown
UniversityName	University of Patras
Matriculation Number	1234

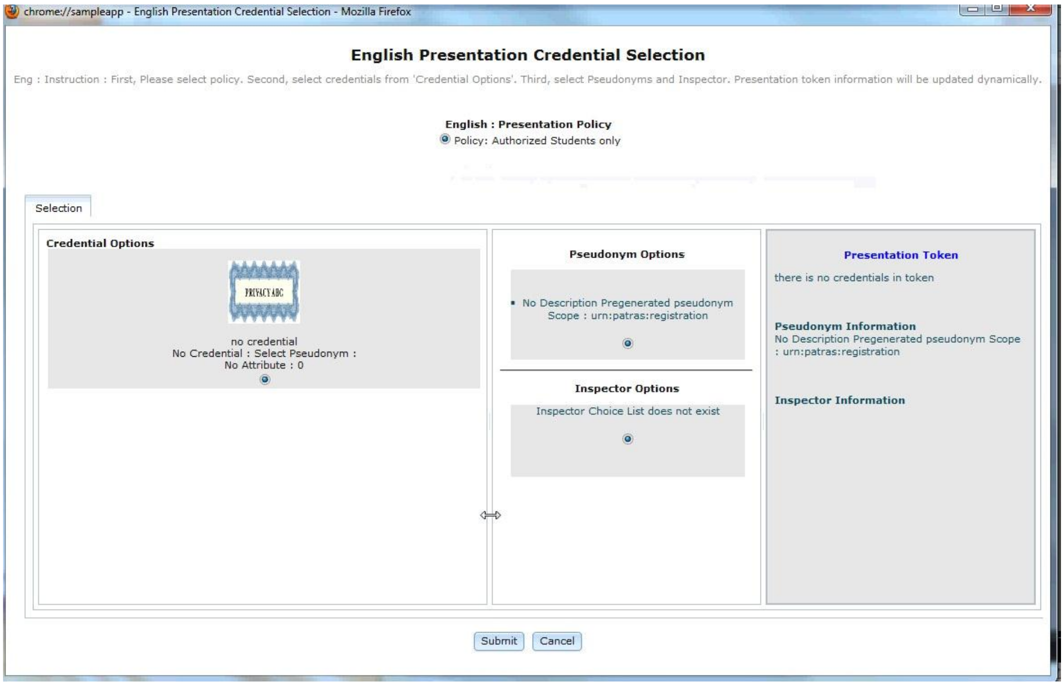
Figure 28: Smart card registration page

How to Register Your Smart Card - Step 7:

Now the “Credential selection: interface pops up and asks to submit your request. You have to select all the following options:

- ☑ Policy: Authorized Students only
- ☑ No credential
- ☑ Pseudonym Options
- ☑ Inspector Options

Press Submit to continue. You will be asked to proceed with the Credential Selection in the other window as shown in **Figure 30**. Click on the OK button.


chrome://sampleapp - English Presentation Credential Selection - Mozilla Firefox

English Presentation Credential Selection

Eng : Instruction : First, Please select policy. Second, select credentials from 'Credential Options'. Third, select Pseudonyms and Inspector. Presentation token information will be updated dynamically.

English : Presentation Policy

● Policy: Authorized Students only

Selection

Credential Options

no credential
No Credential : Select Pseudonym :
No Attribute : 0

Pseudonym Options

- No Description Pregenerated pseudonym Scope : urn:patras:registration

Inspector Options

Inspector Choice List does not exist

Presentation Token

there is no credentials in token

Pseudonym Information

No Description Pregenerated pseudonym Scope : urn:patras:registration

Inspector Information

Figure 29: Credential Selection Window

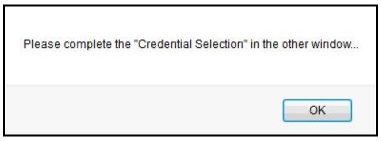
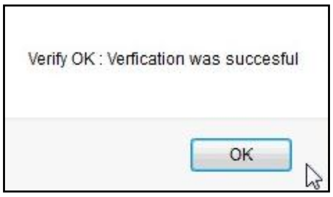

Please complete the "Credential Selection" in the other window...

Figure 30: Request to switch to the window

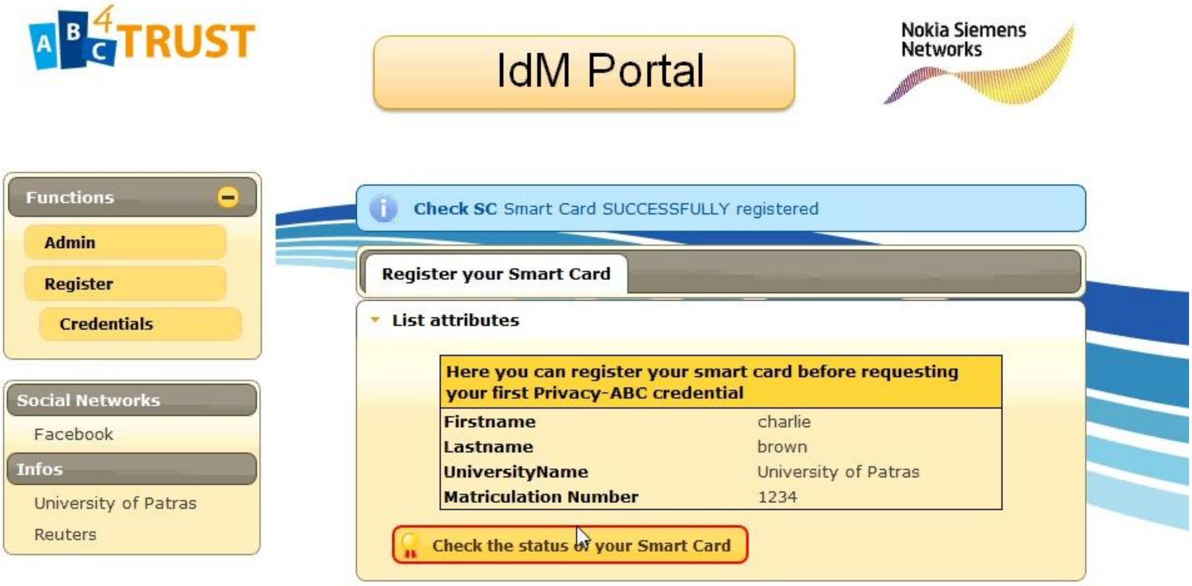
How to Register Your Smart Card - Step 8:

The System authenticates you by using the stored data in your smart card and if authentication is successful you will see a “Verification OK” message (**Figure 31**). If your registration has completed successfully a message will be shown on top of the page (**Figure 32**).



Verify OK : Verfication was succesful

Figure 31: Verification OK



Check SC Smart Card SUCCESSFULLY registered

Here you can register your smart card before requesting your first Privacy-ABC credential

Firstname	charlie
Lastname	brown
UniversityName	University of Patras
Matriculation Number	1234

Figure 32: Successful smart card registration

How to Register Your Smart Card - Step 9:

Now your smart card is registered and you can proceed obtaining your credentials (see Section A.3.3 and A.3.4). You can check the status of your smart card by selecting the "check the status of your smart card " menu in registration web page.

Note:

- **When you want to register at the University and obtain a valid student credential, you have to complete successfully the above registration phase (see section A.3.2) and to possess a valid student Privacy ABC on his smart card.**
- **You have to plug the USB cable of card Reader to your computer and place the SmartCard into the card Reader.**

A.3.2.1 Troubleshooting the SC's Registration

If you cannot access your account at step 4, you have to check and reenter your OTP and your matriculation number.

If you cannot access credential selection menu at step 7, you have to check your smart card connection to your computer via your reader as the Figure 22 shows.

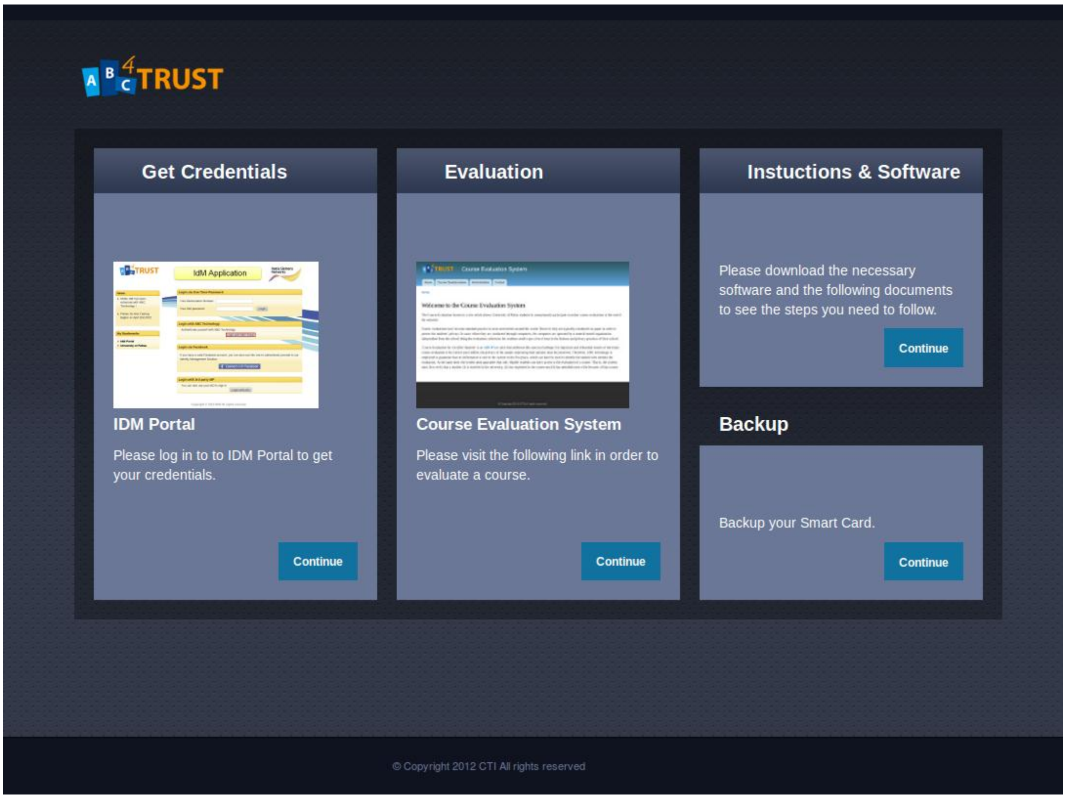
If you cannot receive system's authentication at step 8 or get an error message, you have to check your smart card connection to your computer via your reader as the Figure 22 shows.

If your status of your smart card does not appear as registered, you have to repeat the registration procedure from the beginning.

A.3.3 How to Obtain a University Credential

How to Obtain a University Credential - Step 1:

Visit Patras Portal site at https://ces.cti.gr/Portal/Portal.html. You will see the following interface on your screen. Follow the link for "Get Credential".



Get Credentials

IDM Portal

Please log in to to IDM Portal to get your credentials.

Continue

Evaluation

Course Evaluation System

Please visit the following link in order to evaluate a course.

Continue

Instuctions & Software

Please download the necessary software and the following documents to see the steps you need to follow.

Continue

Backup

Backup your Smart Card.

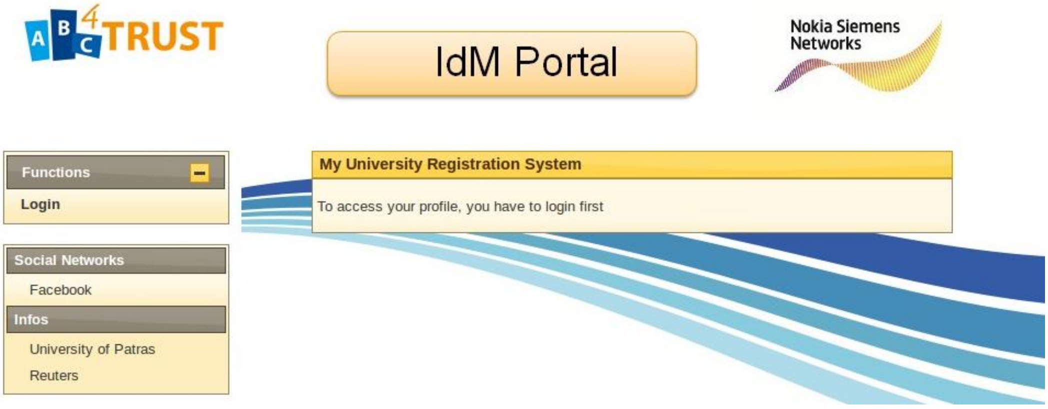
Continue

© Copyright 2012 CTI All rights reserved

Figure 33: Patras Portal

How to Obtain a University Credential - Step 2:

Now you are redirected to IDM Portal welcome page as shown in **Figure 34**. Please click on the "Login" link on the left column of this page.



IdM Portal

Nokia Siemens Networks

Functions

Login

Social Networks

Facebook

Infos

University of Patras

Reuters

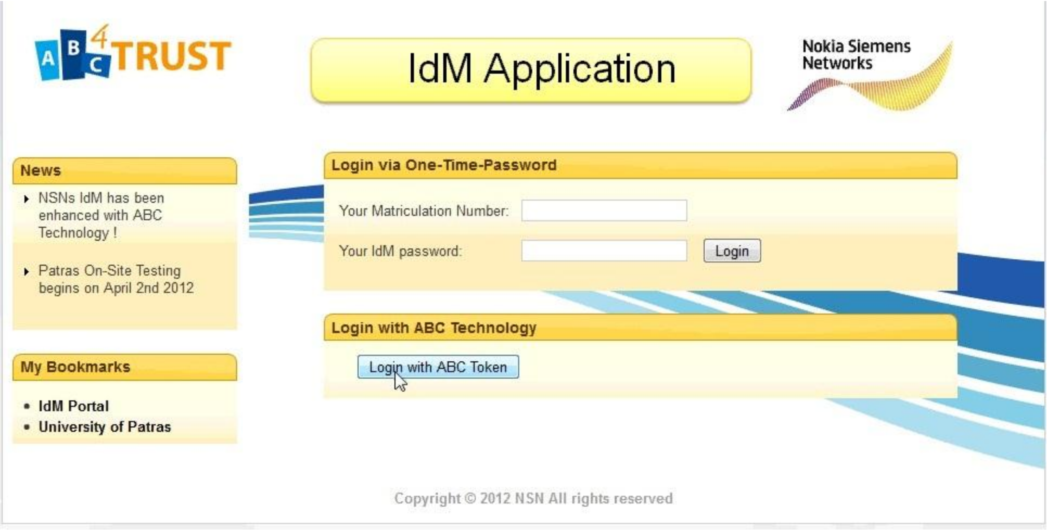
My University Registration System

To access your profile, you have to login first

Figure 34: IdM Welcome Page

How to Obtain a University Credential - Step 3:

You need to login via ABC Technology. Select the '*log in with ABC token*' tab as shown in **Figure 35** in order to be logged in.



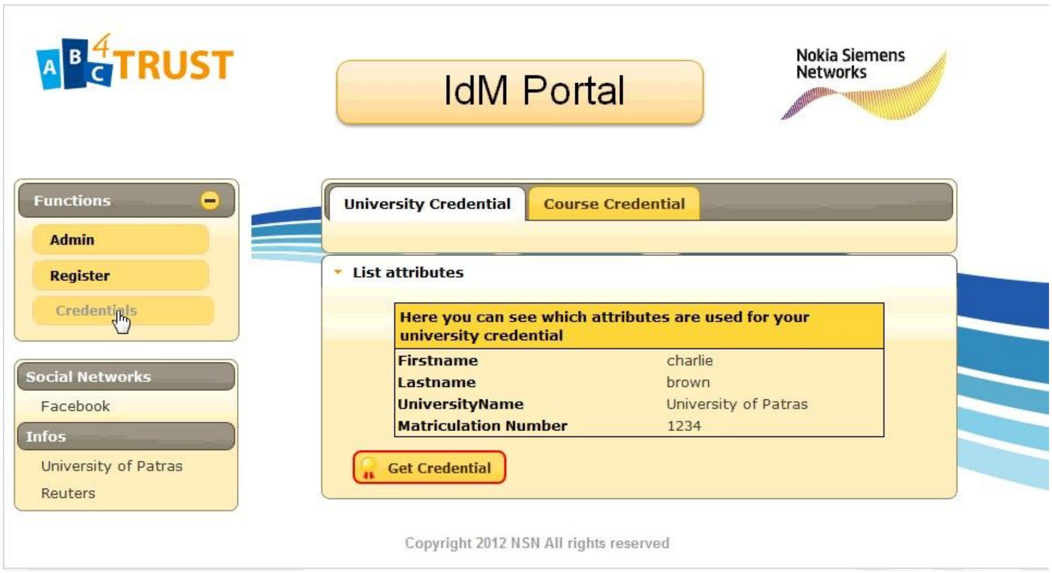
ABC4TRUST
IdM Application
Nokia Siemens Networks
News
NSNs IdM has been enhanced with ABC Technology !
Patras On-Site Testing begins on April 2nd 2012
My Bookmarks
IdM Portal
University of Patras
Login via One-Time-Password
Your Matriculation Number:
Your IdM password:
Login
Login with ABC Technology
Login with ABC Token
Copyright © 2012 NSN All rights reserved

Figure 35: Log in with ABC Token

How to Obtain a University Credential - Step 4:

If the authentication is successful you will see a welcome message (**Figure 26**).

Now you can select “credentials” link in the functions menu of your account page (**Figure 36Figure 27**).

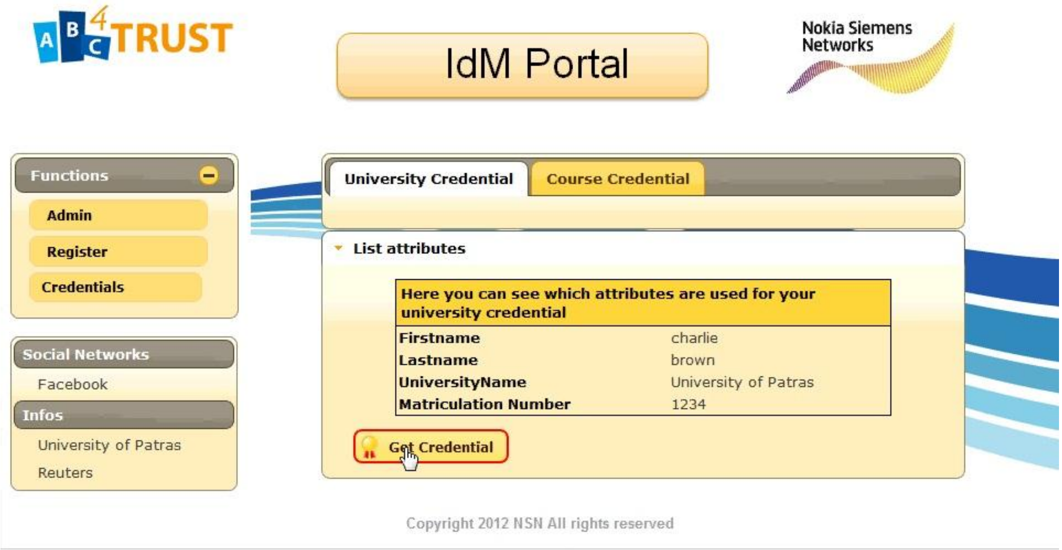


Here you can see which attributes are used for your university credential	
Firstname	charlie
Lastname	brown
UniversityName	University of Patras
Matriculation Number	1234

Figure 36: Credentials Environment

How to Obtain a University Credential - Step 5:

At this point your account page must be similar with the page shown in the figure below. Please click on the link “Get Credential”.



Here you can see which attributes are used for your university credential	
Firstname	charlie
Lastname	brown
UniversityName	University of Patras
Matriculation Number	1234

Copyright 2012 NSN All rights reserved

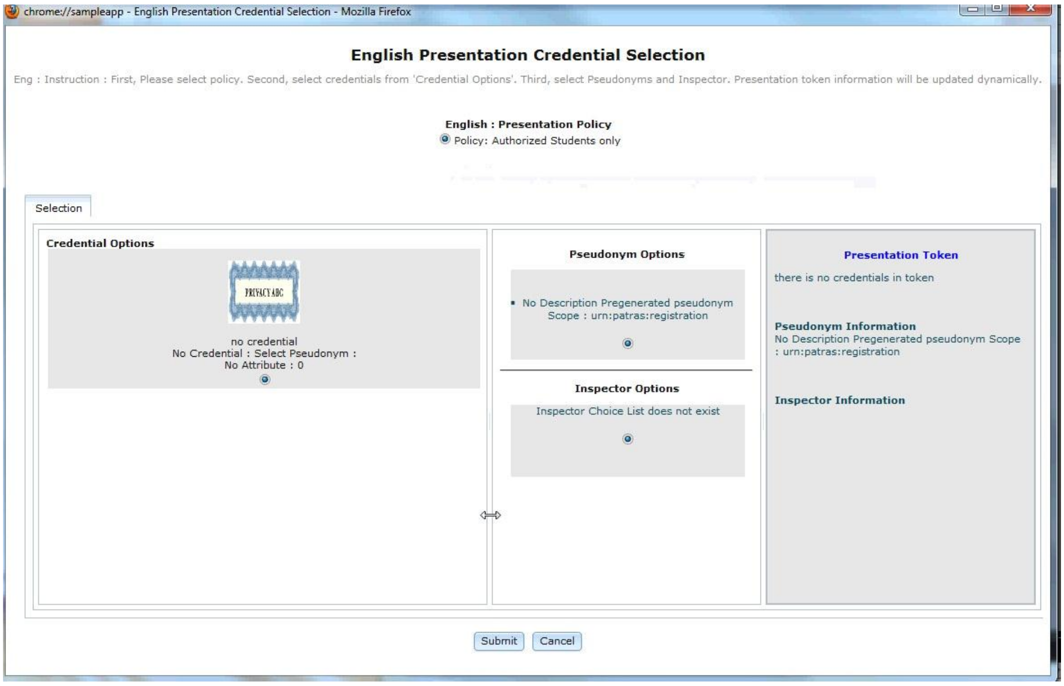
Figure 37: Getting your University Credential

How to Obtain a University Credential - Step 6:

Now the “Credential selection: interface pops up and asks to submit your request. You have to select all the following options:

☑ Policy: Authorized Students only
☑ No credential
☑ Pseudonym Options
☑ Inspector Options

Press Submit to continue. You will be asked to proceed with the Credential Selection in the other window as shown in Figure 39. Click on the OK button.



chrome://sampleapp - English Presentation Credential Selection - Mozilla Firefox

English Presentation Credential Selection

Eng : Instruction : First, Please select policy. Second, select credentials from 'Credential Options'. Third, select Pseudonyms and Inspector. Presentation token information will be updated dynamically.

English : Presentation Policy
● Policy: Authorized Students only

Selection

Credential Options

no credential
No Credential : Select Pseudonym :
No Attribute : 0
●

Pseudonym Options

- No Description Pregenerated pseudonym Scope : urn:patras:registration

●

Inspector Options

Inspector Choice List does not exist
●

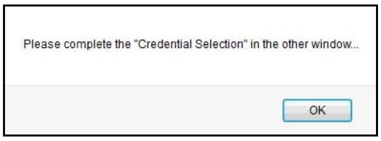
Presentation Token

there is no credentials in token

Pseudonym Information
No Description Pregenerated pseudonym Scope : urn:patras:registration

Inspector Information

Figure 38: Credential Selection Window

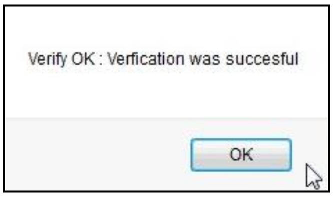


Please complete the "Credential Selection" in the other window...

Figure 39: Request to switch to the window

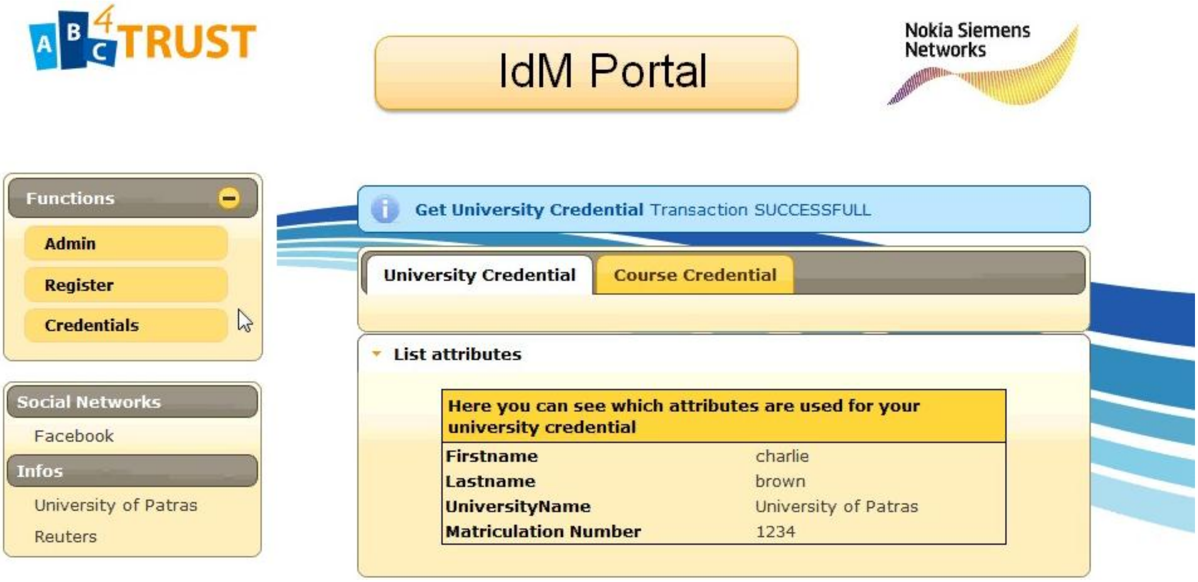
How to Obtain a University Credential - Step 7:

The System authenticates you by using the stored data in your smart card and if authentication is successful you will see a "Verification OK" message (Figure 40). If your University credential is stored in your smart card your credential status will be appeared as shown in Figure 41.



Verify OK : Verfication was succesful

Figure 40: Verification OK



Get University Credential Transaction SUCCESSFULL

Here you can see which attributes are used for your university credential	
Firstname	charlie
Lastname	brown
UniversityName	University of Patras
Matriculation Number	1234

Figure 41: The University Credential obtained successfully

Note:

- **When you want to book a course and obtain a valid course credential, you have to complete successfully the previous registration phase (see Section A.3.2) and to possess a valid student Privacy ABC credential following the steps of obtaining a university credential phase (see Section A.3.3).**
- **You have to plug the USB cable of card Reader to your computer and place the smart card into the card Reader as the Figure 4 shows.**

A.3.3.1 Troubleshooting Getting a University Credential

If you cannot access your account at step 4, you have to check your smart card connection to your computer via your reader as the Figure 22 shows.

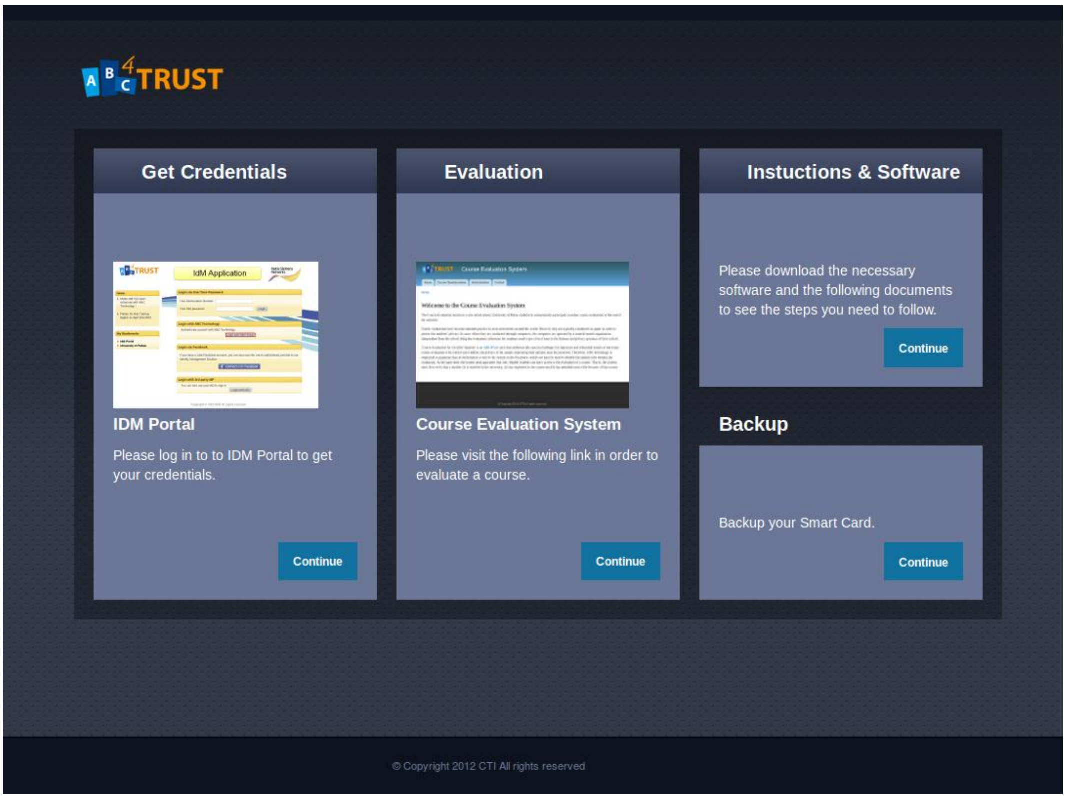
If you cannot receive system's authentication at step 7 or get an error message, you have to check your smart card connection to your computer via your reader as the Figure 22 shows.

If you cannot see a university credential when you check the status of your smart card, you have to repeat this procedure from the beginning.

A.3.4 How to Obtain a Course Registration Credential

How to Obtain a Course Credential - Step 1:

Visit Patras Portal site at https://ces.cti.gr/Portal/Portal.html. You will see the following interface on your screen. Follow the link for "Get Credential".



Get Credentials

IDM Portal

Please log in to to IDM Portal to get your credentials.

Continue

Evaluation

Course Evaluation System

Please visit the following link in order to evaluate a course.

Continue

Instuctions & Software

Please download the necessary software and the following documents to see the steps you need to follow.

Continue

Backup

Backup your Smart Card.

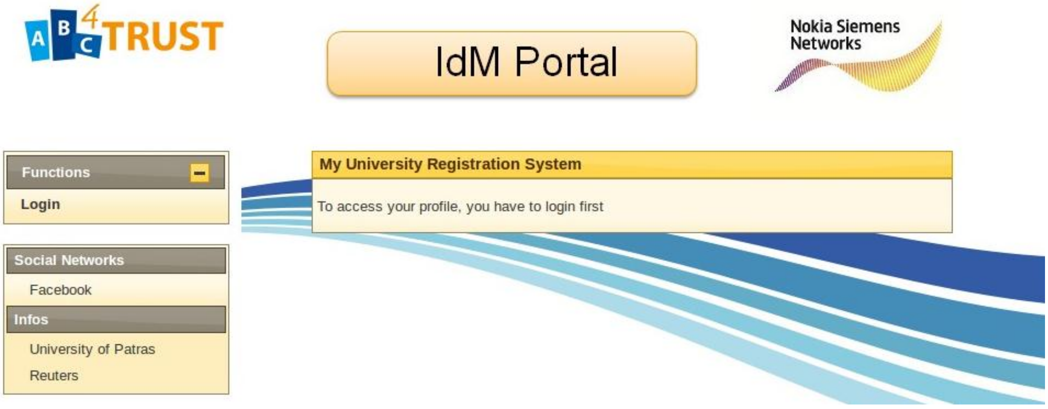
Continue

© Copyright 2012 CTI All rights reserved

Figure 42: Patras Portal

How to Obtain a Course Credential - Step 2:

Now you are redirected to IDM Portal welcome page as shown in following figure. Please click on the “Login” link on the left column of this page.



My University Registration System

To access your profile, you have to login first

Figure 43: IdM Welcome Page

How to Obtain a Course Credential - Step 3:

You need to login via ABC Technology. Select the '*log in with ABC token*' tab as shown in following picture in order to be logged in.

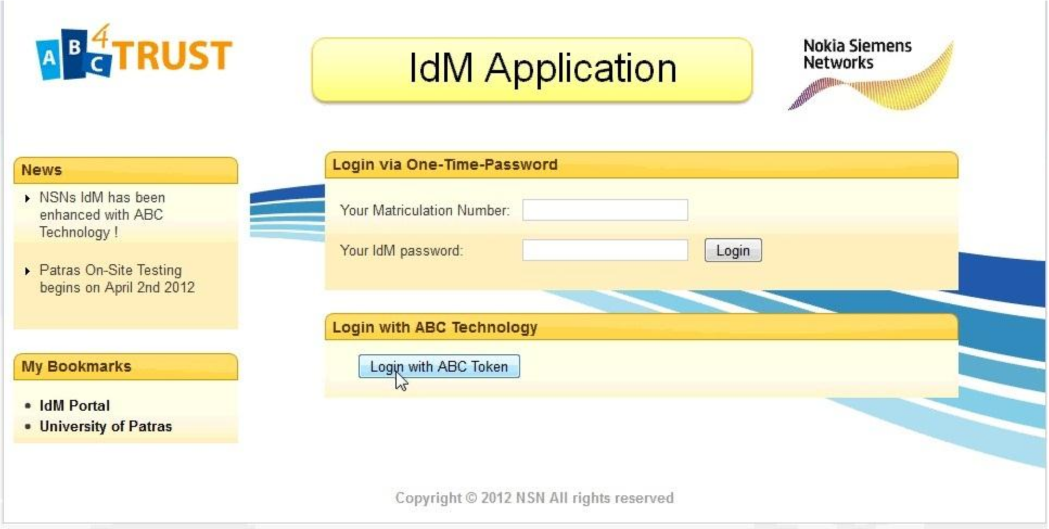

ABC4TRUST
IdM Application
Nokia Siemens Networks
News
NSNs IdM has been enhanced with ABC Technology !
Patras On-Site Testing begins on April 2nd 2012
My Bookmarks
IdM Portal
University of Patras
Login via One-Time-Password
Your Matriculation Number:
Your IdM password:
Login
Login with ABC Technology
Login with ABC Token
Copyright © 2012 NSN All rights reserved

Figure 44: Log in with ABC Token

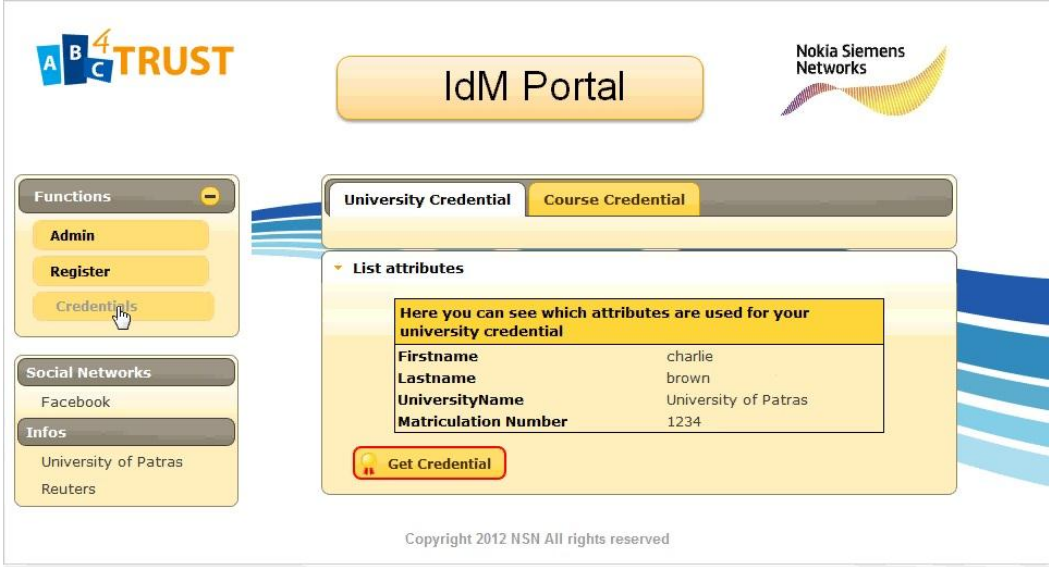
How to Obtain a Course Credential - Step 4:

If the authentication is successful you will see a welcome message (Figure 26).

Now you can access your account information and all your attributes under the “Admin” menu (Figure 27). Finally you can select the “check the status of your smart card” tab in order to view your SC’s status (see Figure 32)

How to Obtain a Course Credential - Step 5:

At your account page select the Credentials tab in the Functions menu (see following picture).

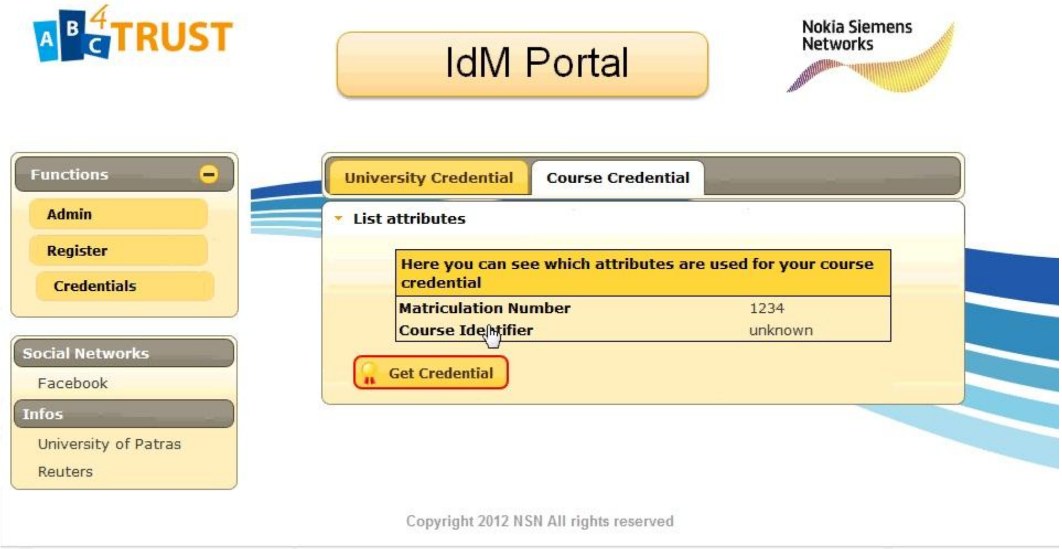


Here you can see which attributes are used for your university credential	
Firstname	charlie
Lastname	brown
UniversityName	University of Patras
Matriculation Number	1234

Figure 45: Credentials Environment

How to Obtain a Course Credential - Step 6:

At this point your account page must be similar with the page shown in the figure below. Please click on the link “Get Credential”.



Here you can see which attributes are used for your course credential

Matriculation Number	1234
Course Identifier	unknown

Figure 46: Getting your Course Credential

How to Obtain a Course *Credential - Step 7:*

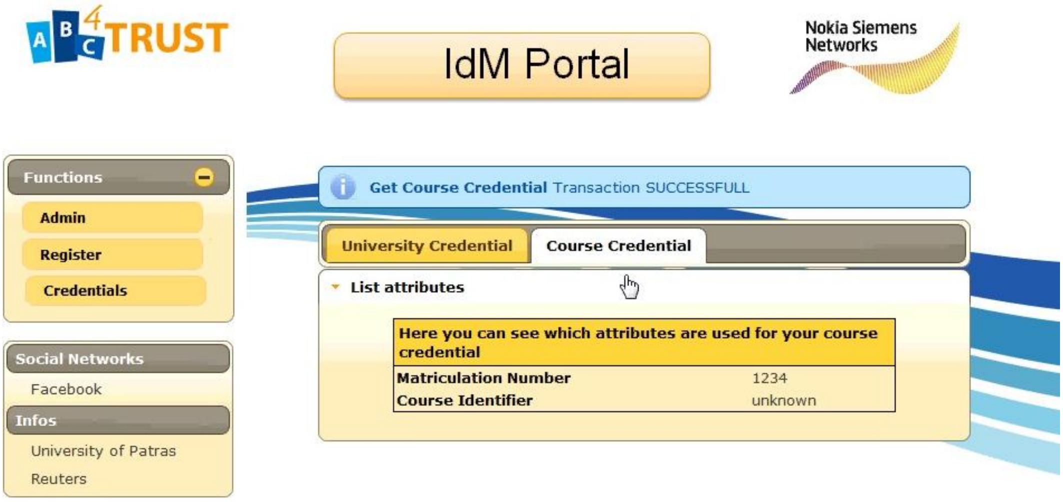
Now the “Credential selection: interface pops up and asks to submit your request. You have to select all the following options:

- ☑ Policy: Authorized Students only
- ☑ No credential
- ☑ Pseudonym Options
- ☑ Inspector Options

Press Submit to continue. You will be asked to proceed with the Credential Selection in the other window as shown in Figure 30. Click on the OK button.

How to Obtain a Course Credential - Step 8:

The System authenticates you by using the stored data in your smart card and if authentication is successful you will see a “Verification OK” message (Figure 31). If your Course credential is stored in your smart card your credential status will be appeared as shown in Figure 47.



Get Course Credential Transaction SUCCESSFULL

Here you can see which attributes are used for your course credential

Matriculation Number	1234
Course Identifier	unknown

Figure 47: Your Course Credential Obtained Successfully

A.3.4.1 Troubleshooting Getting a Course Credential

If you cannot access your account at step 4, you have to check your smart card connection to your computer via your reader.

If you cannot receive system’s authentication at step 8 or get an error message, you have to check your smart card connection to your computer via your reader.

If you cannot see a course credential when you check the status of your smart card, you have to repeat this procedure from the beginning.

A.3.5 How to Obtain Class Attendance Data

Each student can collect his attendance information by waving his smart cart in front of a contactless NFC reader when leaving the lecturing room. NFC reader is responsible for storing attendance data on the students' smart cards during the lecture of a course. NFC reader will be placed in lecture room 15 minutes before 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.

Note:

- ***You must have in your possession a smart card.***
- ***You must have also a smart card reader.***
- ***The class Attendance system is placed in lecture room.***

How to Obtain Class Attendance Data - Step 1:

You have to wave your smart cart in front of a contactless NFC reader when leaving the lecturing room, in order to collect your attendance information. You will hear a voice signal (bit signal) for verifying you that your attendance has successfully stored in your smart card. Your smart card is updated every time you attend a class.

A.3.6 How to Backup Your SC's Data

Each student can back up his smart card data. You must have attended some course lectures and have some attendance information stored on your smartcard. A software component called "User Agent" that runs locally on your PC is triggered every time you want to have access to your data stored on your smart card. User Agent application is responsible for browsing the Privacy-ABCs stored on your smart card or backing up the smart card content on your PC.

Note:

- ***You must have attended some course lectures (see section A.3.5) and must have some attendance information stored on your smart card.***
- ***You have to plug the USB cable of card reader to your computer and place the smart card into the card reader as the Figure 22 shows.***

How to Backup Your SC's Data - Step 1:

You should connect your smart card reader to your PC before starting User Agent application. Then, you must run locally User Agent application on your PC in order to back up the smart card content on your PC.

How to Backup Your SC's Data - Step 2:

The User Agent application requests your PIN in order to unlock the card and you have to enter your PIN.

A.3.7 How to Restore SC's Data

Note:

- ***If you have lost your smart card then you have to declare the smart card loss to the University Registration Office and to get a new envelope and a new smart card.***
- ***You have a backup on your PC.***
- **You have to plug the USB cable of card Reader to your computer and place the new smart card into the card reader as the Figure 22 shows.**

If you lose your smart card then you can declare it lost to the University Registration Office where you can get a new envelope and smart card. You must have a backed up smart card content on your PC in order to be able to restore backed up data from your PC on your (new) SC though User Agent application. Note that the PIN and your password for backup and restore can be selected by the user, thus may be different from the PIN for unlocking the SC.

How to Restore Your SC's Data - Step 1:

You should connect your smart card reader to your PC before starting User Agent application. Then, you must run locally User Agent application on your PC in order to retrieve the smart card content on your PC.

How to Restore Your SC's Data - Step 2:

The User Agent application requests your PIN in order to unlock the card and you have to enter your PIN.

How to Restore Your SC's Data - Step 3:

If your PIN is correct the backuped data is stored on your new smart card.

A.3.8 How to Evaluate a Course

You will be able to participate anonymously in a course evaluation by logging in to the Course Evaluation System via ABC technology. When you want to evaluate a course you need to follow the steps described in this section.

Note:

- ***You must have at your possession a valid student credential and one or more course credentials (following the steps described in Sections A.3.3 and A.3.4).***
- ***You must have attended at least 3 lectures of the course since you have to prove sufficient attendance of a specific course in order to evaluate the course.***
- ***You have to plug the USB cable of card reader to your computer and place the smart card into the card reader.***
- ***You must have installed the ABC User Agent on your computer in order to start the course evaluation procedure.***

How to Evaluate a Course - Step 1:

Plug the USB cable of card reader to your computer and place the smart card into the card Reader as the **Figure 48** shows. Otherwise, you can use the University's card readers, which are located in the computer center.

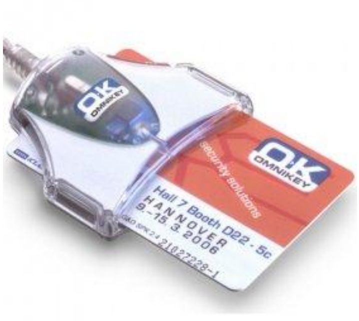
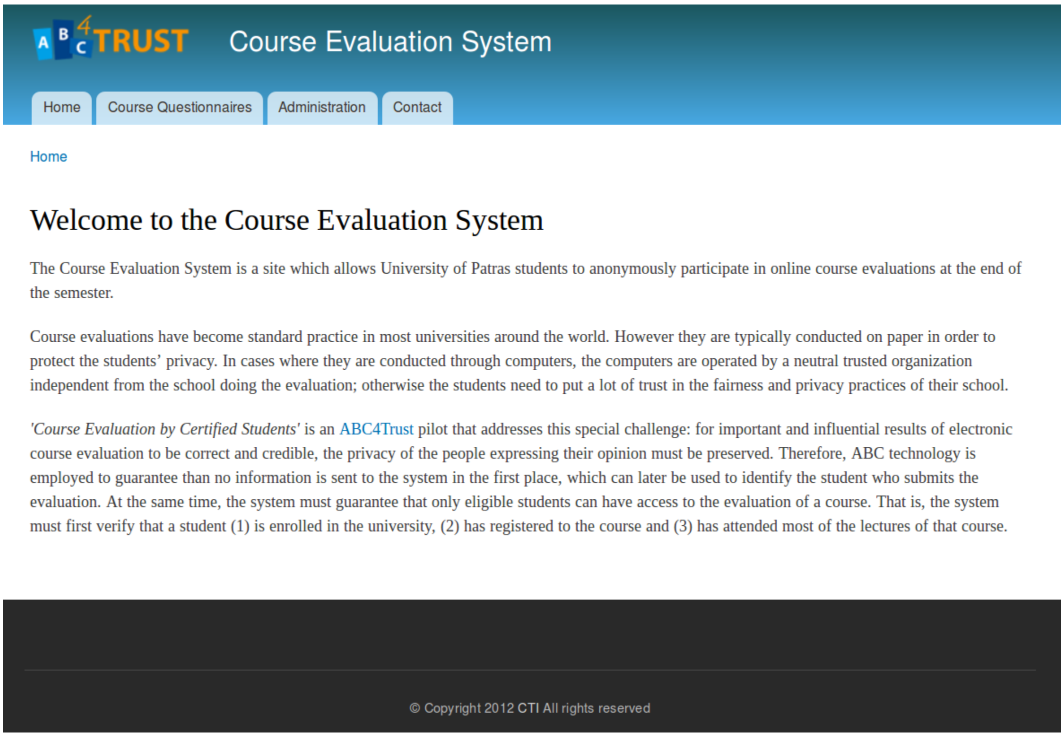


Figure 48: Smart card reader

How to Evaluate a Course - Step 2:

Visit the Course Evaluation System at https://ces.cti.gr/ in order to verify that the Course Evaluation process has begun. In that case, follow the menu tab “*Course Questionnaires”*.



Welcome to the Course Evaluation System

The Course Evaluation System is a site which allows University of Patras students to anonymously participate in online course evaluations at the end of the semester.

Course evaluations have become standard practice in most universities around the world. However they are typically conducted on paper in order 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 school.

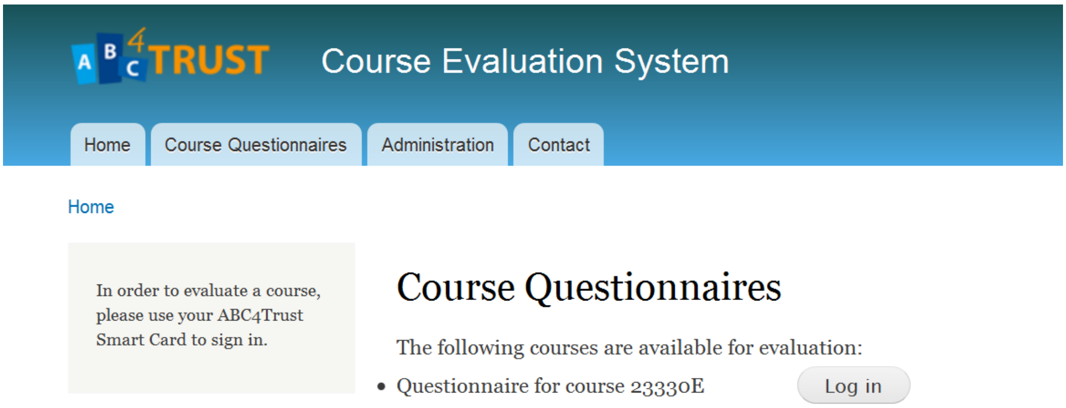
'Course Evaluation by Certified Students' is an ABC4Trust pilot that addresses this special challenge: for important and influential results of electronic course evaluation to be correct and credible, the privacy of the people expressing their opinion must be preserved. Therefore, ABC technology is employed to guarantee 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 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 most of the lectures of that course.

© Copyright 2012 CTI All rights reserved

Figure 49: Course Evaluation System

How to Evaluate a Course - Step 3:

In this page, click on the "*Log in*" button. This calls the Firefox plugin and populates a window where you can choose which credentials to use for the verification process.



In order to evaluate a course, please use your ABC4Trust Smart Card to sign in.

Course Questionnaires

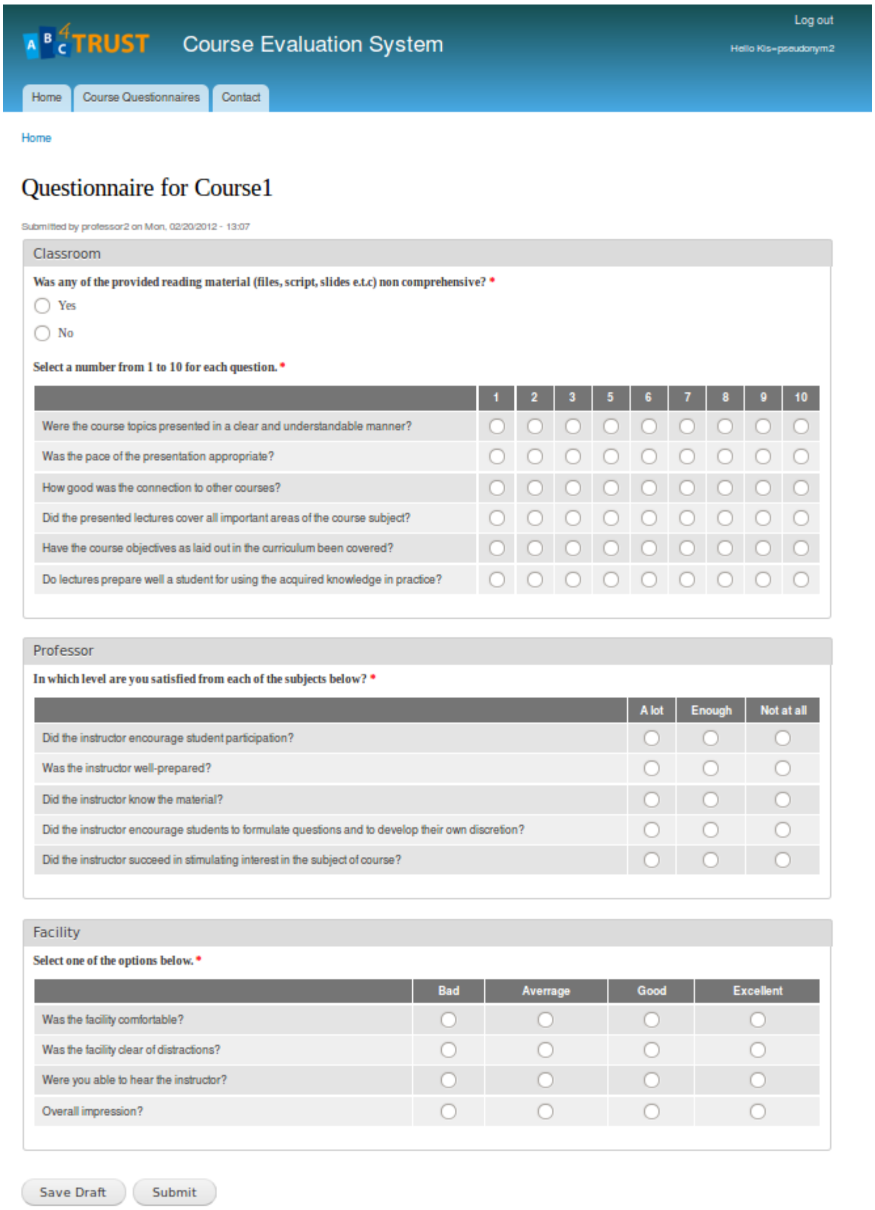
The following courses are available for evaluation:

- Questionnaire for course 23330E

Figure 50: Course Questionnaires Login Page

How to Evaluate a Course - Step 4:

If the verification process is successful the questionnaire appears. In the end of each questionnaire there is a *"Save draft"* button which you can use in order to continue the course evaluation another time and not lose your answers



Questionnaire for Course1

Submitted by professor2 on Mon, 02/20/2012 - 13:07

Classroom

Was any of the provided reading material (files, script, slides e.t.c) non comprehensive? *

○ Yes

○ No

Select a number from 1 to 10 for each question. *

	1	2	3	5	6	7	8	9	10
Were the course topics presented in a clear and understandable manner?	○	○	○	○	○	○	○	○	○
Was the pace of the presentation appropriate?	○	○	○	○	○	○	○	○	○
How good was the connection to other courses?	○	○	○	○	○	○	○	○	○
Did the presented lectures cover all important areas of the course subject?	○	○	○	○	○	○	○	○	○
Have the course objectives as laid out in the curriculum been covered?	○	○	○	○	○	○	○	○	○
Do lectures prepare well a student for using the acquired knowledge in practice?	○	○	○	○	○	○	○	○	○

Professor

In which level are you satisfied from each of the subjects below? *

	A lot	Enough	Not at all
Did the instructor encourage student participation?	○	○	○
Was the instructor well-prepared?	○	○	○
Did the instructor know the material?	○	○	○
Did the instructor encourage students to formulate questions and to develop their own discretion?	○	○	○
Did the instructor succeed in stimulating interest in the subject of course?	○	○	○

Facility

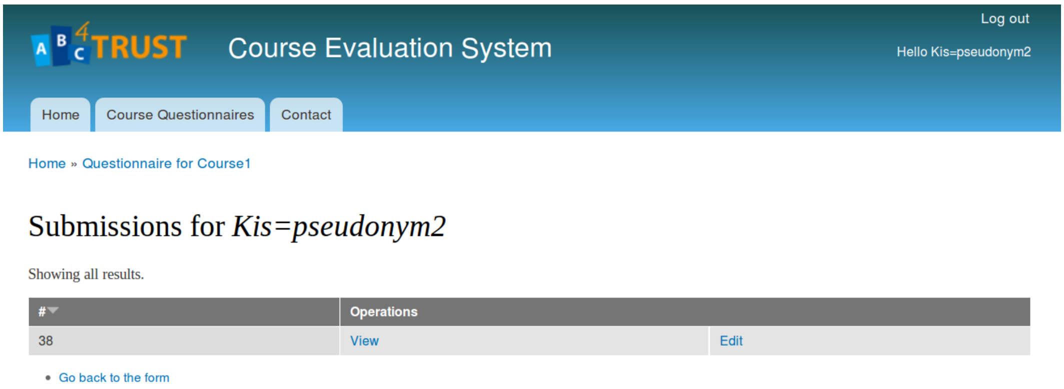
Select one of the options below. *

	Bad	Averrage	Good	Excellent
Was the facility comfortable?	○	○	○	○
Was the facility clear of distractions?	○	○	○	○
Were you able to hear the instructor?	○	○	○	○
Overall impression?	○	○	○	○

Figure 51: Questionnaire form

How to Evaluate a Course - Step 5:

If you have already completed the questionnaire, you can visit your submission so as to edit or view it.



Home » Questionnaire for Course1

Submissions for *Kis=pseudonym2*

Showing all results.

#	Operations	
38	View	Edit

- Go back to the form

Figure 52: Questionnaire Editing Option

How to Evaluate a Course - Step 6:

After finishing the submission just *"Log out"* and pull the card out of the Reader. For any problems or further information you can visit the "*Contact"* page to find the contact details.

A.3.8.1 Troubleshooting for Evaluating a Course

- ⌦ If you cannot log in at step 3 you have to check your matriculation number or to check your smart card connection to your computer via your reader.
- ⌦ If you receive an error message that you have not sufficient attendance, you will not be able to evaluate the course

Appendix B User Consent Form

Computer Technology Institute and Press "Diophantus"

Vasiliki Liagkou
"D. Maritsas" Building, Nikou Kazantzaki street
University Campus of Patras
Rion, PO box 1382
265 00
email:Liagkou@cti.gr
Phone:2610960301 Fax:2610960490

Information sheet related to the pilot deploying Privacy-ABCs within the project ABC4Trust

What is the ABC4Trust project?

The abbreviation “Privacy-ABC” stands for “privacy enhancing Attribute-based Credentials”. Privacy-ABC’s are a technology that enables individuals preserving their privacy whenever they need to identify or register for an Information and Communication Technology (ICT) system. With the extensive distribution of systems requiring a secure authentication or identification of users, in a broad range of scenarios, the users’ privacy is increasingly threatened. Privacy-ABCs allow the user to only reveal the information absolutely necessary for the execution of the required action and thus respect the privacy of the individual. The project ABC4Trust (Attribute Based Credentials for Trust) is a research and development project funded by the European Union under its 7th Research Framework Program (FP7) as part of the ICT Trust & Security programme. Having started in November 2010 with duration of four years, the project aims at achieving a more thorough understanding of Privacy-ABC by enabling the deployment in practice and their federation in different domains.

The University pilot

The ABC4Trust project launches a pilot deploying Privacy-ABC’s at the

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

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

No identifying information about the student will be collected during the evaluation phase.

Each participating student will receive a set of credentials matching the use case of the pilot. In this context, the term “credential” means that this is a single piece of information that might be necessary for the student’s eligibility of participating in a specific course evaluation. An example would be the proof that the owner of the credential is indeed student of the department offering the course, or that the student is registered to the course under evaluation and has attended a sufficient number of lectures. Credentials will be stored on a smart card provided by CTI. The credentials on the smart card are protected by a PIN known only to the participant.

How can I participate as student?

For the duration of the trial, each participating student will be given a smart card and a card reader to connect with the student’s own personal computer at home. The smart card will contain the student’s credentials (e.g. name, matriculation number, registered courses, etc.). Whenever a student visits a predefined course, his/her course presence can be registered on the personal smart card. So, these cards become a tool for the students to collect the attendance information and use them to access the online course evaluation system via the internet at home. The ABC System provides to the student an online interface between the browser and her smart card. For this reason, it employs a software component called “User Agent” that runs locally on the student’s PC. This software component is triggered every time a participant is required to provide data stored on her card and asks for consent. Moreover, it enables the student to browse the Privacy-ABCs stored on the own smart card, delete Privacy-ABCs and locally backup Privacy-ABCs. Details for the handling of the smart card, the User Agent software, how to obtain credentials or to participate in the poll are explained step by step in the pilot handbook available at the pilot’s portal page: https://ces.cti.gr/Portal/Portal.html

Treatment of personal data

For the registration process the following information will be transmitted from the university to CTI for exclusive use within the pilot:

First- and last name

Matriculation number

Name of the University (for this pilot: “University of Patras”)

Name of the department (for this pilot: “Department of Computer Engineering and Informatics”)

Courses the student is subscribed to (for the pilot: “Distributed Systems I”)

The named data is securely stored by CTI in the University Registration System for the purpose of issuing respective credentials to be stored locally on the smart cards of the participants and to re-issue credentials in case of lost cards. In addition, access to this data may become necessary for CTI to ensure and measure the functionality of the pilot system and for tracking and remove errors. Participants have the possibility to access and rectify data stored in the University Registration System online, or by contacting CTI.

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

Retrieved credentials are stored on the smart card under the control of the participant and accessible only with the PIN.

During the polling process, only the necessary information is provided to access the system. Identifying information such as first and last name or the matriculation number are not necessary and will not be revealed during this process. Privacy-ABCs allow verifying a participant's attributes with cryptographic means, e.g. verifying that the participant is member of the university and registered for the particular course without disclosing name or matriculation number. Further details on the functionality of Privacy-ABCs can be found at: www.abc4trust.eu.

Once the evaluation period is closed, the results will be aggregated and passed on to the lecturer as statistics. Further transfer or publication will only be made in aggregated form.

The personal data in the University Registration system will be deleted 3 months after the end of the semester. The anonymous polling results will be used by ABC4Trust for the evaluation of the pilot software and deleted at latest six month after the end of the evaluation has been closed.

User consent, revocation, consequence of not consenting

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

All personal information provided by the students will be treated carefully and confidential. It will be stored securely and will not be used or disclosed to third parties without the student's explicit consent. Since this pilot is part of scientific research project, aggregated and anonymised data will be used to complete the research work of this project as well as it will be used for academic purposes, like the publication of scientific proceedings; for drafting various informative reports, containing presentations of graphs and statistics that will be publicly available.

Contact details of the data controller:

Computer Technology Institute and Press "Diophantus"

"D. Maritsas" Building, Nikou Kazantzaki street

University Campus of Patras

Rion, 26500

Contact Person: Vasiliki Liagkou

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

email:Liagkou@cti.gr

Tel:2610960301

More information about the project can be found at:

www.abc4trust.eu

More information about the system is contained in the user manual to be found at:

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

Consent form for the Patras pilot participation in the ABC4Trust project

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

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

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

CTI is assisted by ABC4Trust project partner Nokia Siemens Networks GmbH & Co. KG (NSN), Munich, Germany, in setting up, running, and administering the University Registration System (data processor). For this it may become necessary to grant employees of NSN physical or online access to the University Registration System for administration purposes, validation of the system’s functions as well as tracking and removing of errors. Under these circumstances your personal data may become known to NSN personnel.

All information provided by you regarding yourself will be stored securely and will not be used or disclosed to third parties without your explicit consent. Your opinion about the lecture which you provide as part of this trial will be anonymous and not linkable to your person. For academic purposes, like the publication of scientific proceedings, reports, or presentations anonymised and aggregated graphs and statistics will be made publicly available. Your personal data (name, matriculation number) will be stored not longer than two months after the end of the trial. This consent form will be securely kept with CTI until 6 months after the end of the project.

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

Please express your consent regarding the usage of your personal data in the trial as described above by ticking the box below. You can revoke this consent any time by contacting Vasiliki Liagkou who will facilitate your withdrawal from the trial

□ By ticking this box, I indicate my willingness to voluntarily take part in the trial. I have read and understood the terms and conditions of this trial.

Date: ________ Name: ___________________________ Signature: ______________________

Please print your name

Please give the filled registration and consent forms to: Vasiliki Liagkou

Appendix C Student's Questionnaire

C.1 Classroom

- Was any of the provided reading material (files, script, slides e.t.c) non comprehensive?
- Were the course topics presented in a clear and understandable manner?
- Was the pace of the presentation appropriate?
- How good was the connection to other courses?
- Did the presented lectures cover all important areas of the course subject?
- Have the course objectives as laid out in the curriculum been covered?
- Do lectures prepare well a student for using the acquired knowledge in practice?

C.2 Professor

- Did the instructor encourage student participation?
- Was the instructor well-prepared?
- Did the instructor know the material?
- Did the instructor encourage students to formulate questions and to develop their own discretion?
- Did the instructor succeed in stimulating interest in the subject of course?

C.3 Facility

- Was the facility comfortable?
- Was the facility clear of distractions?
- Were you able to hear the instructor?
- Overall impression?

C.4 Course Subject

- Were you interested in the subject of the course?
- Will the subject of the course be important in your job life?
- Was the course material relevant to your interests?
- How do you find the difficulty level of the course for its semester?

C.5 Questions on the person of the student

- Have you regularly prepared for class ?
- Have you regularly done follow-up course work during the semester?
- Have you regularly done assigned / suggested homework (if applicable) ?
- Have you contributed to class with answers, questions or comments in discussions?

C.6 Questions after the Course Exam

- Questions for all students:
    - Would you describe the exam to be fair compared to the content of the class?
    - Would you describe the exam to be fair in respect to the time granted for the assignment?
    - Questions for students with good results (better than average grades in Greek system)
    - How may the course can be improved ?

- Questions for students with bad results (worse than average grades in Greek system and failing)
    - Is there something that could be improved about the course that would have helped you to better success?