D5.1 Scenario Definition for both Pilots

Souheil Bcheri, Norbert Götze, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Yannis Stamatiou, Katalin Storf, Peder Wängmark, Harald Zwingelberg

Editors:	*Norbert Götze (Nokia Siemens Networks), Yannis Stamatiou (Computer Technology Institute)*
Reviewers:	*Pascal Paillier (CryptoExperts), Christian Paquin (Microsoft)*
Identifier:	*D5.1*
Type:	*Deliverable*
Version:	*1.0*
Date:	*04/02/2012*
Status:	*Final*
Class:	*Public*

Abstract

In this document we provide a high level description of the use case scenarios that we have chosen for implementation in the two pilots that will be conducted in order to assess the ABC4Trust framework. We also describe the roles of the agents that are involved in the pilots as well as their responsibilities with respect to the handling of information processed during the conduct of the pilots. Furthermore, in this document we describe the characteristics and requirements of the two pilots so as to drive, appropriately, engineering and architectural decisions in other work packages that will provide the necessary software support and expertise to the pilots. Our effort was towards delineating the requirements that are common separately from the ones in which the pilots differ so as to start building the common denominator elements of the pilots that will be implemented once for both pilots.

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

Members of the ABC4TRUST consortium

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

List of Contributors

Chapter	Author(s)
Executive Summary	Yannis Stamatiou (CTI)
Introduction	Yannis Stamatiou (CTI)
First Chapter	Christoforos Raptopoulos (CTI), Souheil Bcheri (EDOC)
Second Chapter	Norbert Götze (NSN), Harald Zwingelberg (ULD), Katalin Storf (ULD)
Third Chapter	Norbert Götze (NSN), Souheil Bcheri (EDOC), Peder Wängmark (EDOC), Harald Zwingelberg (ULD)
Fourth Chapter	Norbert Götze (NSN), Vasiliki Liagkou (CTI), Apostolis Pyrgelis (CTI), Christoforos Raptopoulos (CTI), Harald Zwingelberg (ULD)
Fifth Chapter	Souheil Bcheri (EDOC), Götze Norbert (NSN), Yannis Stamatiou (CTI), Harald Zwingelberg (ULD)
Sixth Chapter	Yannis Stamatiou (CTI)
Seventh Chapter	Yannis Stamatiou (CTI)
Eighth Chapter	Yannis Stamatiou (CTI), Harald Zwingelberg(ULD), Christoforos Raptopoulos (CTI)

Executive Summary

The ABC4Trust project's main objective is twofold: (i) the definition of a unified reference architecture for systems deploying privacy-enhancing Attribute-based Credentials (Privacy-ABCs) and (ii) the development of an open reference implementation of a full ABC system that will be integrated into two complete real pilot applications that will provide feedback to the reference architecture and implementation results. These will be the first pilots of ABC deployments in real application environments for collecting feedback on the deployment of ABC systems.

The project will gather practical experience with ABC systems in two specific environments: (i) the protection of the anonymity of children in a school environment located in Sweden and (ii) remote, anonymous course evaluation within universities by eligible students in Greece. The first challenges in deploying a full ABC system in these two domains are to clearly describe the target application scenarios and define the resulting set of requirements which are the two main goals of this deliverable.

Our efforts in the deliverable are primarily focused on defining, clearly, the main scenarios and use cases that will be handled by the pilot application systems in the two different pilot contexts of the school and the university. From these scenarios we extract the requirements that will have to be fulfilled by the reference implementation of ABCs as well as the complete pilot application systems. We have tried to keep the definitions and requirements at a high level but keep a balance between having too much detail and, thus, placing constraints at an early stage to the work done in the reference implementation part of the project and having too few details, thus providing very limited information about the pilot application requirements to the implementation work. More details about the chosen scenarios and technical decisions are being, continually, inserted in two living documents maintained by consortium members involved in the reference implementation and the pilots which are called *High Level Technical Design* (HLTD) documents and which expand the information provided in the present project deliverable. Its content will serve as input for upcoming public deliverables. This separation enabled us to provide, formally (through the deliverable), a clear description of the chosen scenarios and their requirements at an early stage and then be able to expand the implementation details gradually as the implementation work on the core components of the ABC system advances.

In this document we also give two tables which show the kind of proofs that will be required to be performed on the pilot related credentials in order to fulfill the requirements of the pilot scenarios. Such a table will guide WP4 (reference implementation of an ABC system), WP6 (system for the school pilot) and WP7 (system for the university pilot).

Finally, in this deliverable we also define the roles of the involved (in the pilots) stakeholders in both the school and the university pilots in order to carry out the defined scenarios. We assign all the roles that are prescribed in deliverable D2.1 [DAACT] (the ABC architecture definition document) to partners and discuss the respecting responsibilities of the partners in the context of each pilot.

The output of this deliverable, along with the HLTD documents, will feed WP4 which is responsible for delivering the reference implementation that will handle the more general requirements of ABC systems set forth by WP2 as well as the pilot related requirements as prescribed in the present deliverable. More details and scheduling information about the two pilots will be provided in deliverables D6.1 and D7.1 of the pilots work packages WP6 and WP7 respectively.

Table of Contents

Introduction 11

1 Objectives of the pilots 12

1.1 Objective(s) of the Söderhamn Pilot 12
1.2 Objective(s) of the Patras Pilot 13

2 Definition of Roles 15

2.1 ABC Roles 15
2.2 Legal Roles 16

3 Söderhamn: Community Interaction among Pupils 19

3.1 Architecture 19
3.2 ABC System Setup 20
3.3 Scenarios 21

3.3.1 Counselling 21
3.3.2 Restricted Chat Room 22
3.3.3 Political Discussions 22
3.3.4 Sharing Documents 23
3.3.5 An Emergency Situation 23

3.4 Privacy-ABCs 23

3.4.1 credSchool 24
3.4.2 credSubject 24
3.4.3 credClass 24
3.4.4 credRole 25
3.4.5 credGuardian 25
3.4.6 credChild 25
3.4.7 Proofs about Credentials 25

3.5 Data Flows 26

3.5.1 Obtaining the School Credential 26
3.5.2 Viewing User's Attributes 30
3.5.3 Inspection 31
3.5.4 Restricted Area 32

3.6 Role Mapping 34

3.6.1 Mapping of ABC roles 34
3.6.2 Mapping of legal roles 36

4 Patras: Course Rating by Certified Students 46

4.1 Architecture 46

4.2 ABC System Setup 48
4.3 Scenarios 49
4.3.1 Obtaining the University/Course Registration Credential 49
4.3.2 Obtaining Class Attendance Data 49
4.3.3 Backup and Restore of Class Attendance Data 50
4.3.4 Revoking a Student's Privacy-ABCs 50
4.3.5 Course Evaluation 50
4.4 Privacy-ABCs 51
4.4.1 credUniv 51
4.4.2 credCourse 52
4.4.3 credAttendance 52
4.4.4 Proofs about Credentials 52
4.5 Data Flows 53
4.5.1 Obtaining the University/Course Registration Credential 53
4.5.2 Obtaining Class Attendance Data 58
4.5.3 Course Evaluation 59
4.6 Role Mapping 61
5 Requirements 67
5.1 Generic Requirements 67
5.2 Söderhamn Requirements 68
5.3 Patras Requirements 70
6 Glossary 72
7 Acronyms 77
8 Bibliography 79

Index of Figures

Figure 1: High Level Architecture of the Söderhamn Pilot 19
Figure 2: Bootstrap/Obtaining first privacy-ABC (a) 26
Figure 3: Bootstrap/Obtaining first privacy-ABC (b) 27
Figure 4: Login to School Registration System via ABC Technology (a) 28
Figure 5: Login to School Registration System via ABC Technology (b) 29
Figure 6: Obtaining auxiliary Credentials after successful Login 30
Figure 7: Viewing Attributes stored in IdM DB after successful Login 31
Figure 8: Inspection 32
Figure 9: Restricted Area (a) 33
Figure 10: Restricted Area (b) 34
Figure 11: High Level Architecture of the Patras Pilot 46
Figure 12: Bootstrap / Obtaining first Privacy-ABC (a) 54
Figure 13: Bootstrap/Obtaining first Privacy-ABC (b) 55
Figure 14: Login to University Registration System via ABC Technology (a) 56
Figure 15: Login to University Registration System via ABC Technology (b) 57
Figure 16: Obtaining credCourse after successful Login 58
Figure 17: Obtaining credAttendance 59
Figure 18: Course Evaluation (a) 60
Figure 19: Course Evaluation (b) 61

Index of Tables

Table 1: ABC Roles Description 16
Table 2: Legal Roles Description 18
Table 3: Matching of legal roles 45
Table 4: ABC Role Mapping for the Course Rating by Certified Students Pilot 62
Table 5: Legal Role Mapping for the Course Rating by Certified Students Pilot 66

Introduction

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

The aim of ABC4Trust is to deepen the understanding in ABC technologies, enable their efficient/effective deployment in practice, and their federation in different domains. Towards this end, the ABC4Trust project aims to run the first ever pilots of ABC deployments in production environments. Thus, this will be the first time real user feedback on ABC systems will be collected. ABC4Trust will gather practical experience with ABC applications in two specific environments.

Two pilots will be conducted:

The School Pilot: This will be a pilot concerning the use of Privacy-ABCs in a Swedish school environment (in Söderhamn) to provide trusted identification while simultaneously protecting the privacy and anonymity of pupils in social network applications that require it to meet the requirements of local (in this case Swedish) authorities. EDOC will be responsible for the deployment of the School pilot.

The University Pilot: This will be a pilot concerning the use of Privacy-ABCs for online course evaluation in the Computer Science department of the University of Patras, in Greece. CTI will be responsible for the deployment of the University pilot.

Having these two specific pilots will give the opportunity to test Privacy-ABC's use and performance with two user groups of differing skills and needs. These pilots will provide feedback of distinct value to the developers of the reference implementation.

This deliverable will define the basic scenarios for the University and the School pilot. It will also define the roles in these two pilots and will present the corresponding high level functional and system requirements. Furthermore, it will provide a high level presentation of the architecture of the systems that will be deployed in the pilots as well as the corresponding credential formats.

1 Objectives of the pilots

In this section we discuss, at a high level, the main objectives of the two pilots of the ABC4Trust project. Our aim is to set the scene for what the pilots will do in terms of the deployment of ABC4Trust technologies in two different real application domains and what the basic scenarios are.

The two pilot applications have as a common goal to evaluate the ABC technologies of the ABC4Trust project and provide feedback to the reference architecture and implementation that will be provided to the pilots. The scenarios are chosen so as to evaluate as many as possible ABC features and functionalities in real application environments.

In a later deliverable (D5.2, month 19) the common denominator elements (i.e. characteristics and requirements) of the two pilots will be extracted and documented. That deliverable will comprise the mapping of the scenarios to the reference architecture, integration of the pilot systems with the reference implementation of WP4 as well as the software/hardware requirements of the pilots.

1.1 Objective(s) of the Söderhamn Pilot

Söderhamn pilot will realize a trial where young pupils (youngsters and teenagers of both sexes) in an anonymous and privacy preserving way can communicate with other pupils and with school health personnel (doctors, nurses and other coaches). Pupils will be able to ask very private questions about their sexuality, weight and other physical and health problems.

More specifically, the objectives for the Swedish School pilot are to:

1. Schedule and conduct a research on a web based school community application.
2. Define success criteria and detailed plans for the school community application.
3. Provide feedback to the architecture and reference implementation WPs.
4. Provide evaluation results to Users, Identity Service providers, and Application Providers.

The background of the pilot is that Swedish schools of today are mainly using the Internet for communication between teachers, pupils and parents. User names and passwords are used to identify the users. A big threat against the privacy of the students are unauthorized access or access to sensitive personal information such as individual plans, presence reports, grades, exam results and other important functionality such as chat and forum available at the school portal.

The Swedish pilot will develop a new Web Based School Community Application to be used for chat communication, counseling, political discussions and exchange of sensitive and personal data between pupils, parents and school personnel such as teachers, administrators, coaches, nurses etc. The application will be based on a new concept called Restricted Area (See chapter 3 “The Restricted Area Concept”).

The major challenges are that the School Community Application needs to offer many different functionalities needed by the many different scenarios such as chat, counseling, political discussions, document sharing etc. It needs to be flexible enough to meet different requirements from many different stakeholders such as pupils, parents and school personnel. And finally it needs to be very secure in order to meet requirements from authorities and legislation.

The main scenarios for the Swedish pilot are

- Communicating and socializing via
    - Chat

  - Forum
  - Wall
- Political discussions
- Counseling with health personnel (counselors, social workers, nurses, coaches)
- Sharing and access to important documents (absence reports, individual plans, grades, exam results)

The basic requirements for the Swedish pilot are:

- To allow users to communicate with other Users which are either online or offline and to exchange sensitive and non-sensitive information in different formats between different parties with different access policies.
- The users are in charge of what they reveal and can therefore choose to either remain completely anonymous (and use pseudonyms) or to prove their real identity. This can be done at anytime and anywhere in the application and can be different from time to time.
- The users are in charge and can choose to whom they prove their identity. They can disclose their full name, e.g., "Claudia Hugosson", or they can prove some parts of their attested identity attributes such as "Girl", "Age 9-12" or "A girl, age 10-11" (selective disclosure).
- The users can choose what attributes they want to prove and to whom.

Participants in the pilot are:

- 400 pupils and their parents/guardians.
- 7th-9th grader (12-16 years old pupils).
- 80 teachers and other school personnel.
- 3 principals.

1.2 Objective(s) of the Patras Pilot

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

More specifically, the objectives for the University pilot are:

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

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

With respect to (2), the University trial of the ABC4Trust framework will define the success criteria compared to the classical process based on paper evaluation forms. The Student Evaluation scenario of the ABC4Trust framework will a) allow the students to evaluate courses, b) automatically archive the evaluation results in electronic form, and c) offer the possibility of using strong cryptographic tools to ensure student anonymity and data confidentiality.

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

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

CTI will conduct two 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. There will be two trials: one in the first month of the fall semester of the year 2012 to evaluate a course whose examination will be performed in January 2013 and spring semester of the year 2013, to evaluate a course whose examination will be performed in June2013. This will assure that the second 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. In order to assure that everything will operate as expected, CTI will conduct a small scale experimental trial with 3-5 students equipped with smart cards in a mock up pilot setup. This will be when the reference implementation is ready by the end of April 2012.

2 Definition of Roles

In this section we discuss the roles of the pilot stakeholders with respect to the Swedish and Patras pilots. We have two different types of roles: (i) ABC roles, which pertain to the ABC related functionalities and (ii) legal roles, which pertain to the protection of personal information items of the pilot participants.

2.1 ABC Roles

In this subsection, we discuss the ABC related roles in the following table. For each role, we give a brief role definition and some comments which clarify the functioning of the role.

ABC Roles	Definition	Commentary
Issuer	The Issuer generates and provides credentials containing Attributes to the User. An Issuer issues credentials to Users, thereby vouching for the validity (timing) and correctness (values) of the information contained in the credential with respect to the User to whom the credential is issued.	On request, the Issuer generates the credential during the issuance protocol and provides it to the User (usually on the basis of a legal relationship). Depending on the use case, the information to be contained in the credential may be provided by the User or the Issuer already holds the respective information. The legal relation between Issuer and User may be based on a plenitude of relations, such as a service contract only for the purpose of attaining a certificate but also citizenship, membership (municipality, university, and schools) or employment, etc.
User	The User is issued the credentials while interacting with the Issuer enabling her to provide proof of certain attributes towards the Verifier.	The User acts in different roles. She receives credentials of the Issuer and provides a proof for certain requested attributes plus (in some cases) information needed for inspection. If the authentication is done in course of concluding a contract the User also fulfils the contractor's identification or authentication requirements for the conclusion of the contract and might give her declaration of intent. Regularly the User also holds

ABC Roles	Definition	Commentary
		legal role 'Data Subject', see Section 2.2 below).
Inspector	The Inspector reveals the identity or other encrypted attribute values of a User (e.g. lifting anonymity) upon legitimate request of the Inspection Requestor. For this, the Inspector has to examine the legitimacy according to the inspection grounds.	The Inspector, its inspection policy and its privacy policy must be known by all parties prior providing the proof. The Inspector should preferably be independent from the User. The independence may be achieved by appropriate technical or organisational safeguards.
Inspection Requestor	Entity requesting an inspection from the Inspector, asserting that inspection is compliant with the inspection grounds specified or is legally required.	In most cases this will be the Verifier, but also may be the police, or other legally authorised entity. The Inspection Requestor may have other roles at the same time.
Inspection Receiver	The entity receiving the reply of the Inspection.	This entity must specify the inspection grounds. The Inspection Receiver may be identical with other roles, namely the Inspector.
Revocation Authority	A Revocation Authority is responsible for revoking issued credentials, so that these credentials can no longer be used to generate a Presentation Token.	In most cases the Revocation Authority may be the Issuer.
Revocation Requestor	The entity that initiates the request to the revocation authority to revoke a certain credential.	The Revocation Requestor may be the Issuer.
User Agent	The entity that represents the human User and manages her credentials.	

Table 1: ABC Roles Description

2.2 Legal Roles

In addition to the ABC roles described above in Section 2.1 the applicable data protection law defines several other roles. It is necessary to mention these roles at this place as the law binds legal consequences to the natural persons or legal persons (entities) that hold a particular role. Depending on the processing step at stake and the relation between the parties the entities involved in the pilot may take different roles (see [Zwi11]).

Generally it will be referred to the European legal framework for Data protection.[1] However, as ABC4Trust will pilot the technology at the Greek university of Patras and the school in Söderhamn the Greek[2] and Swedish[3] national Data Protection Laws are applicable to the processing of data done by entities seated in the respective legislations, Art. 4 Para. 1 (a) of Directive 95/46/EC.

The following legal roles are or might be relevant for the legal evaluation of the ABC4Trust pilots.

Legal Roles	Definition	Commentary
Data Subject	An identified or identifiable natural person to whom personal data relates to. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to her physical, physiological, mental, economic, cultural or social identity.	The Data Subject is the legal terminology describing the target of protection of the European privacy legislation. In the ABC4Trust context the User will be data subject in most cases. However, depending on the use case it is imaginable that the User is not a natural person but either a legal entity (company) or even a machine. In these cases the two definitions do not match.
User (ePricacy Directive)	User means any natural person using publicly available electronic communications service, for private or business purpose, without necessarily having subscribed to this service.	To avoid confusion with the ABC role "User" the participants in the pilot will be referred to as data subjects unless the passage explicitly deals with the d-privacy directive. In this case it will be indicated.
Data Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for her nomination may be designated by national or Community law.	Here processing means any operation or set of operation which is performed upon personal data, whether or not by automatic means (defined in Directive 95/46/EC). E.g. such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This includes the action of anonymisation or

[1] For the legal evaluation Directive 95/46/EC (Data Protection Directive) and Directive 2002/58/EC (E-Privacy Directive) set the legal foundations for all EU member states. The definitions of the roles are identical to the definitions of the respective directives.

[2] Namely Law 2472/1997 which is the enactment of the Data Protection Directive, and Law 3471/2006 being the enactment of the E-Privacy Directive). Both laws are available in an English translation: http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL.

[3] English translations of the Swedish "Personal Data Act (1991:204)" and the Personal Data Ordinance (1998:1191)" are available online: http://www.datainspektionen.se/lagar-och-regler/patientdatalagen/

Legal Roles	Definition	Commentary
		pseudonymisation of personal data, even if after such action the data may no longer constitute personal data.
Data Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.	
Recipient	A natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.	The role of the recipient is if interest for legally evaluating the transmission or disclosure of personal data including disclosure within the organisation of a data controller and towards a data processor ([GolSch10], § 3 BDSG para. 51).

Table 2: Legal Roles Description

3 Söderhamn: Community Interaction among Pupils

3.1 Architecture

The general architecture of the ABC4Trust pilot as it will be deployed in Söderhamn is depicted in Figure 1 below and further described within this section.

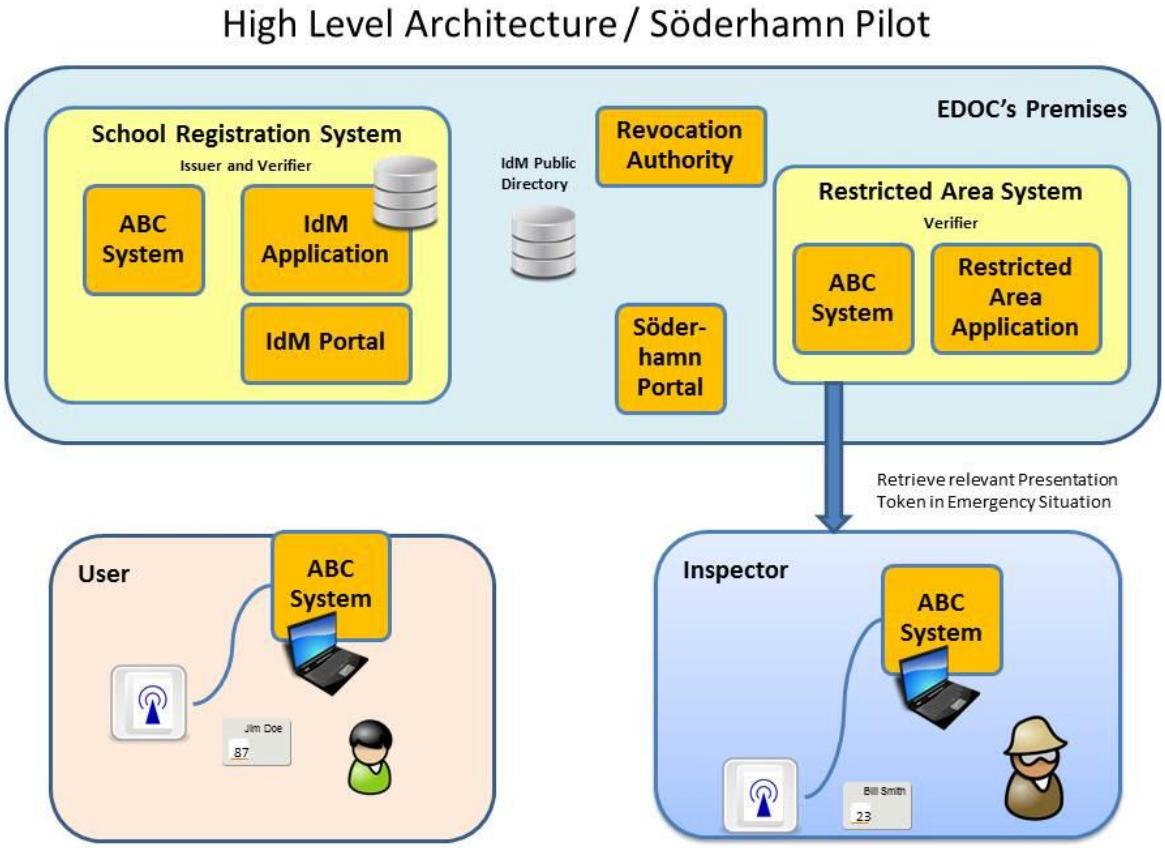

Figure 1: High Level Architecture of the Söderhamn Pilot

As can be seen from the previous figure, the architecture of the Söderhamn pilot is based on various components. These components have different functionalities and roles based on the scenario and use case definition of this pilot. Next, we describe the functionality and the characteristics of each high level component that is presented on the architecture figure.

School Administration: This is the basic component, used for issuing and verifying pupils' credentials. The School Administration Office is responsible for adding and updating information.

Restricted Area System: This is the main component used for protecting the access to a resource or a service from non-eligible pupils. It is responsible for giving grant access to those Users (i.e. pupils) that satisfy certain properties.

Inspector: The inspector is a trusted entity like School inspector board, that can trace the user or pupil who created a presentation token by revealing attributes that were originally hidden from the Restricted Area System. This action takes place upon legitimate request of the school personnel, a guardian, a pupil or law enforcement. Finally, the inspection reply is provided by the school inspection board or law enforcement.

Söderhamn Portal: This is an information portal for the pupils through which they can be instructed how to operate the system. It will also provide the necessary links to the other components of the system (e.g. School Administration, Restricted Area System). This portal will be public.

User Home Application: This application will run locally on pupil's PC and will provide an interface between the pupil and her smart card. It employs a user agent application that is responsible for the communication between the browser and the smart card. Moreover, it gives pupils the opportunity to browse the credentials stored on their smart card, delete credentials or backup the smart card content on their PC.

3.2 ABC System Setup

The ABC System Setup includes the following: The school will provide all needed information about the users such as their names. The ABC4Trust project will provide the necessary hardware in terms of Smartcards and the respective readers. The Smartcards are then finalized by printing the name of the users and by personalizing the chip of the card to install the needed ABC application and web-server certificates. There will be no photos on the cards. The school will also prepare the IdM System to contain attributes such as name, civic registration number, class etc. which are required for generating the corresponding credentials. The school administrators will identify the users and handout the card readers and the personalized cards with the corresponding envelop to the users.

Preparation of IdM Database

- The school administrator (with the help and assistance from Eurodocs) prepares the IdM (Identity Management) System to contain a minimal subset of attributes (name, civic registration number, …) of all users who will take part in the trial

The preparation and personalization of the smart cards

- The smart cards will be prepared off-line
  - ➢ to contain the 'ABC application(s)'
  - ➢ to contain the web-server certificates of all trusted communication partners
  - ➢ with a graphic personalization which includes:
    - ✓ a 'smart card number' which maps to the number on the sealed envelope
    - ✓ the name of the authorized holder
- The ABC Token Presentation requires 'unlocking' the smart card via PIN which will be handed out to the user via sealed envelope
- The sealed envelope will also contain a PUK

Distribution of user information, terms of use and contract signing

Before any cards can be distributed each user will get printed information about the ABC4Trust and the goals and purposes of this EU-project. This information will be written in a simple and non-technical way to be understandable by the pupils. The users will also receive pilot specific information

such as the terms of use, access policies, revocation and the conditions for the inspection. Each user needs to accept all the conditions by signing a legal document hereafter called the pilot contract.

Pupils will be asked to take all the documents, the information including the pilot contract, back to their guardians and ask them to sign the contract. When the contract is signed the Pupils will be allowed to proceed with the next step which is the Distribution of smart cards and card readers.

Parents that are willing to participate in the pilot will be asked to sign their own contract.

School personnel participating in the project will also need to sign the pilot contract.

Distribution of smart cards and card readers

- The user shows her personal identification documents to the school administrator and signs a legal document thereby accepting the privacy and usage policies
- The user obtains a smart card, a contactless smart card reader and a sealed envelope containing the initial PIN and a PUK for her smart card
- The administrator hands out a slip of paper containing the one-time-password for the initial login of the user
- The administrator maps the user's dataset in the IdM system to the smart card ID and to the one-time-password

A small set of exemplary Users will take part in the Söderhamn pilot without smart cards. They will use personal computers. The goal is to prove, that physical tokens are no prerequisite for using ABC-technology.

3.3 Scenarios

The different Swedish scenarios will involve pseudonymous community access and social networking or anonymous student counselling or medical advice. ABC technology allows combining strong authentication and privacy protection into one solution. The proposed community will protect the users (pupils, guardians and school personnel) identity against theft while protecting their anonymity and privacy. On one hand, pupils will be able to identify themselves to access restricted chat rooms and restricted information. On the other hand they will be able to remain anonymous when asking private and sensitive questions from school personnel, while assuring that school personnel communicate only with authorized pupils of the respective school or class.

3.3.1 Counselling

In this scenario a pupil that needs counselling will be able to contact authorized professionals regarding physical and other health related problems. In a normal case the pupil is the one that initiates such a counselling communication. A counselling session begins immediately if the school personnel are available online. Otherwise the communication can be performed asynchronously (send a message and receive an answer later).

In this scenario there will be no counselling for parents/guardians. But it will be possible for the pupil or the counsellor to invite a parent/guardian to join a counselling session if necessary and if it’s accepted by the pupil.

Attributes can be requested and exchanged during a session. Exchanged attributes can be anonymous (a girl, age 10-14) or uniquely identifiable (name, civic registration number etc.). Counselling can be done individually one-to-one or in group.

3.3.2 Restricted Chat Room

This scenario describes two different use-cases which are almost identical.

1. A person that wants to chat with other users by entering a chat room (group).

2. A person that wants to chat with another person in a private chat room (one-to-one)

A precondition is that some public Restricted Area with chat functionality has been created by school administrators or other authorized school personnel. Other Restricted Areas with chat functionality have been created by other users such as pupils, parents, teachers etc.

Each Restricted Chat Room has its own access policy stating who is entitled to access/enter the chat room. The administrator of the chat room (normally the one who did create the chat room) can add one or several access policies indicating the users or groups of users that are allowed to enter and access the chat room. Access policies can also be a mixture of individuals and groups. For example:

- Only for 12-13 years
- Only for girls 12-13 years
- Only for boys 12-15 years
- Only for class 7A
- Souheil Bcheri
- Teachers
- Nurses OR Souheil Bcheri

The user that navigates to the chat section of the website will see lists and groups of all public and available Restricted Areas that have chat rooms functionality activated. The user will also see the access policy (e.g. Age 14-15 years) for each Restricted Chat Room. The user selects a Restricted Chat Room and the system (i.e. the Verifier) will validate if the user (his presentation token) meets the required access policy for the chat room. Upon success the user joins the chat room and is now able to send and receive messages. If the user does not meet the access policy (presentation policy) she will be notified and will see the result of the policy testing.

Anytime during a chat session the user can choose to expose any of her attributes.

3.3.3 Political Discussions

Political discussions are very important in a modern and democratic society. Anonymous political discussions can encourage some people to dare express their opinion in order to have a free discussion about sensitive subjects.

Political discussions are performed using Restricted Areas with the chat and forum functionality activated. And the Restricted Area configuration settings allow anonymous sign in and no exchange of attributes is allowed. When the actual political discussion begins the Restricted Area system will of course validate that each user trying to enter a discussion meets the access policy of the Restricted Area. The user is still anonymous. She will not be able to exchange any attributes even if she wishes to do so. The inspection functionality (the possibility of revealing the identity of the user that misbehaves) is disabled in the political discussions scenario.

3.3.4 Sharing Documents

The school is producing many documents (exam results, grades, individual development plans etc.) that need to be shared with or distributed to the pupils and their parents/guardians. Documents are produced outside the system and can be in any format (MS-Word, PDF, Excel etc.).

Document sharing is possible at any Restricted Area (RA) that has the "Document Sharing" functionality activated. Every user that is included in the access policy will of course be able to upload documents to a Restricted Area. The uploaded documents are then available and accessible by all users that are included in the access policy and have access to the RA. By default a Personal Restricted Area exists for every user in the system.

Important documents will be uploaded to the user's personal Restricted Area. The user who has access to her own personal Restricted Area can sign in to her RA and get access to all uploaded documents.

Personal Restricted Areas have as a default setting only one person included in its access policy. But this can of course be changed to include e.g. the pupil's guardians. Documents are easily uploaded to Personal RAs simply by knowing the Name and/or Personal Number of the owner. Users such as school personnel not included in the access policy will send a request for uploading documents. The document will be pending until the owner of the Restricted Area accepts the request and the document will then be uploaded to the RA.

Sometimes teachers or other school personnel need to upload grades, exam results and other documents to a pupil's Personal Restricted Area. As every pupil or user is the only one that can access her own Personal RA there is an on-going discussion about the possibility to allow all school personnel the possibility to upload documents to all Personal Restricted Areas per default. But this is not finalised.

3.3.5 An Emergency Situation

In an emergency situation such as the protection from immediate danger for life or health (e.g. amok) there are built in mechanisms in the ABC technology allowing an inspector to reveal the identity of a user.

The conditions, the reasons and the definition of an emergency situation will be clearly defined in the contractual relationship beforehand (and might even be public). Before the pilot start the reasons and the definition of emergency will be finalized.

The following steps are to be made if the inspector (TTP[4]) has revealed the identity of a user.

- Depending on the situation, once appropriate, the user concerned must be informed.
- The act of inspection must be securely logged and made known to some predefined control organ.

Alternatively we could stipulate the inspection requires that at least two persons or more act jointly (e.g. principal and data protection office). This is called The School Inspection Board.

3.4 Privacy-ABCs

A Privacy-ABC contains attributes about the user. Attributes have the form of key=value (First name =Souheil). Users can have multiple attribute values for one and the same attribute (e.g. Role). In the following text, we call this kind of attribute 'multiple'. On top of that, Users can have only one attribute value for a specific attribute (e.g. Last name). In the following text, we call this kind of attribute 'single'.

[4] TTP: Trusted Third Party (see Acronyms)

Attributes of the type single can have only one value per person: First name=Souheil, Last name=Bcheri, Civic Registrations Number =640512-3875.

Attributes of the type multiple can have several values for the same person: a teacher can be a coach. The same person can have several roles e.g. a teacher and a coach. (Role= Teacher, Role = Coach). A pupil might study two or more subjects (subject=English, subject=German, Subject=French), A parent might have two or more children in the school.

In order to be able to take care of attribute of the type multiple without leaking information intentionally or unintentionally to the Verifier we had to distribute the attributes on different credentials.

In the case when a teacher changes a role, the old credential needs to be revoked and a new credential with the new role will be issued.

When using the credentials the user can combine different attributes from different credentials into one single presentation token.

3.4.1 credSchool

This credential contains the civic registration number which is unique identity of the users. The same credential also contains all basic attributes of the user. For technical reasons we had to use additional credentials for attributes that can have multiple values.

- First name
- Last name
- Civic Registration Number (age can be extracted from this attribute)
- Gender
- School (In this case it will only be one value/the Söderhamn school: Norrtullskolan)
- Revocation handle

3.4.2 credSubject

Every credSubject credential attests exactly one subject that a pupil is studying. If a pupil is studying n subjects she will possess n credSubject credentials.

- Subject
- Revocation handle

An Attribute value for ‘Subject’ can be e.g. ‘Maths’ or ‘History’ or ‘English’ or ‘French’ or ‘Spanish’, etc.

3.4.3 credClass

This credential contains the class, the grade and the school year that the user belongs to. The year is added to this credential to make it possible to differentiate between different classes and grades between each year of study. A person that belongs to the 7th grade in the year 2011 will probably belong to the 8th grade the next year 2012.We also added additional letter to the grade to differentiate between the different classes within the same year and grade. This credential will make it possible for the administrators of the Restricted Area to add on specific class (class=7A-2011) to the access policy or to add all classes in the 7th grade (Grade=7-2011).

- Class
- Revocation handle

An example attribute value for ‘Class’ can be e.g. ‘7A-2011’.

3.4.4 credRole

The credential contains all the different roles that exist in the Swedish school trial. This not only includes the role of all kinds of school personnel but also the role of pupil or guardian. Every credRole credential attests exactly one role a specific User has. If a User has n roles she will possess n credRole credentials; one for every role.

- Role
- Revocation handle

An Attribute value for 'Role' can be e.g. 'Pupil' or 'Nurse' or 'Teacher' etc

3.4.5 credGuardian

This credential indicates the identity of the pupil's guardians (parents). A pupil can have one or several guardians. If a pupil has n guardians she will possess n credGuardian credentials; one for every guardian.

- Guardians (e.g. Parents)
- Revocation handle

An Attribute value for 'Guardian' can be e.g. '19640512-3875'

3.4.6 credChild

This credential indicates the identity of the guardian's children. The same Guardian (parent) can of course have one or several children in the school. If a guardian has n children she will possess n credChild credentials; one for every child.

- Child
- Revocation handle

An Attribute value for 'Child' can be e.g. '19990111-1234'

3.4.7 Proofs about Credentials

Pupils of Söderhamn School will be issued credentials that certify a number of facts about them (e.g. their age, their classes, their parents, their school name etc.), allowing those with proper credentials to anonymously participate in chat rooms for various purposes (e.g. pupils communication, health and political counseling).

Depending on the use case, the access policy of the Restricted Area visited and the choice of the user, different credentials will be used to proof different attributes or parts of attributes. A pupil entering a Restricted area with Chat functionality and an access policy allowing only girls will of course have to use CredSchool in order to proof her gender. A pupil that wants to access a Restricted area to join a political discussion will use CredSchool to proof that she belongs to the school. A parent that wants to read the grades or absence reports for her own child have to use her CredChild in order to get access to the Restricted are that have this requirements in its' access policy.

It's also possible to use a combination of credentials if the Restricted has an access policy that requires different attributes. To access a chat room for all girls in Class 9B the user needs to use CredSchool and CredClass.

3.5 Data Flows

In this section we give a detailed description of the basic scenarios data flows between architecture entities.

3.5.1 Obtaining the School Credential

When a user wants to receive their first school credential, the user browses the Söderhamn Portal which redirects him to the School Registration System login page. The student can now log in using the one-time-password (OTP) provided in set up phase. Figure 2 presents the corresponding data flows.

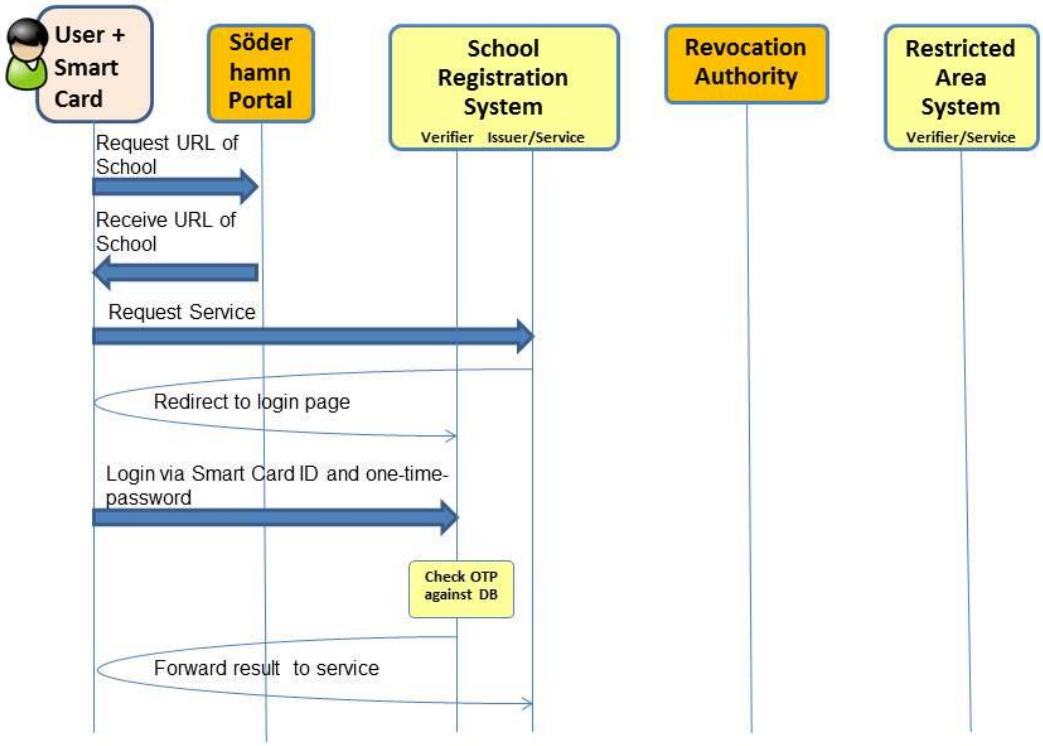

Figure 2: Bootstrap/Obtaining first privacy-ABC (a)

At the next step the user initiates an issuance protocol and a valid Privacy-ABC is stored on her smart card. Figure 3 gives a detailed description of the data flows needed in order to get the credSchool Privacy-ABC.

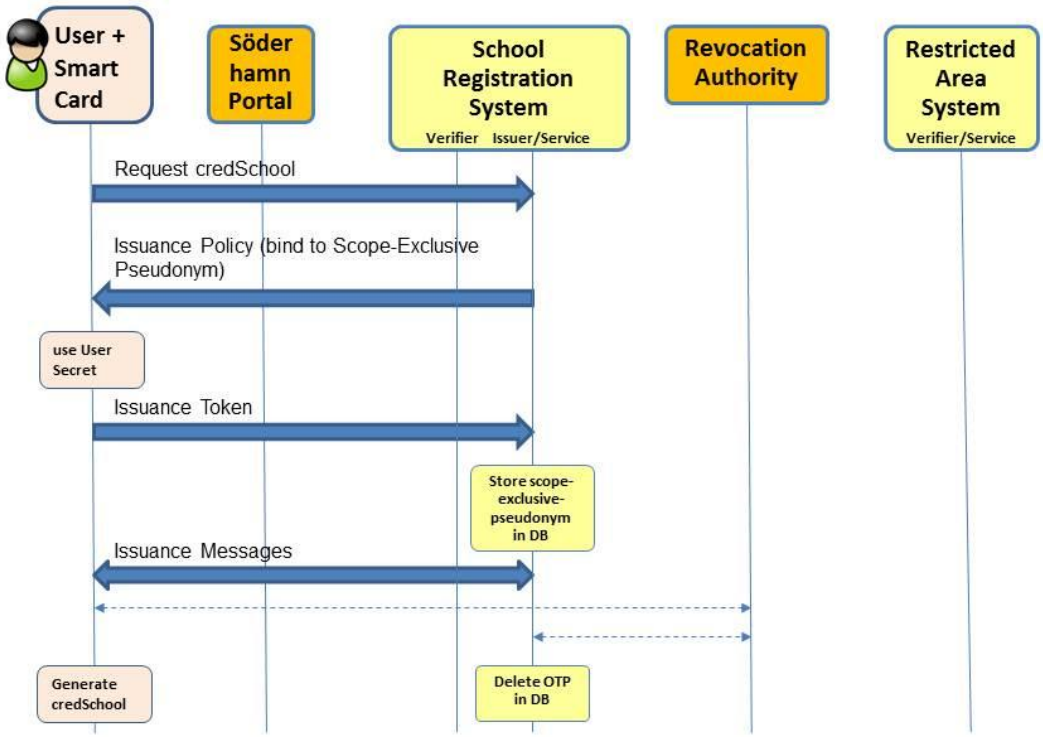

Figure 3: Bootstrap/Obtaining first privacy-ABC (b)

When a user wishes to login to the School Registration System using ABC technology she browses the Söderhamn Portal and gets redirected to the School Registration System. Figure 4 gives an overview of the data flow that ends with the retrieval of the Presentation Policy.

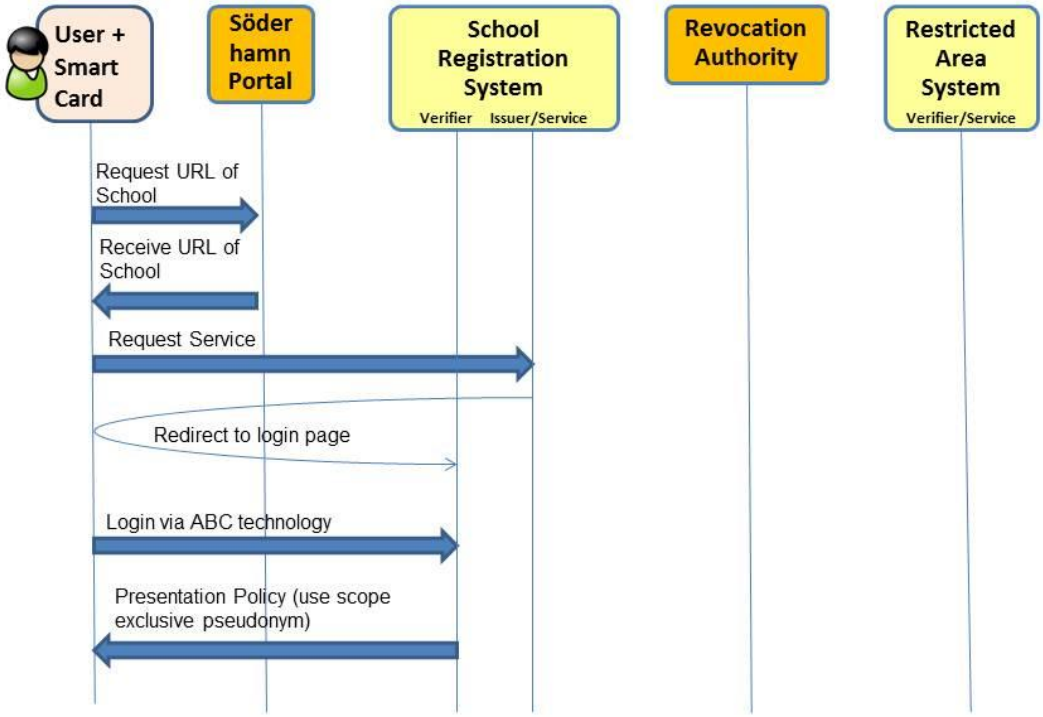

Figure 4: Login to School Registration System via ABC Technology (a)

After the user retrieved the Presentation Policy from the School Registration System she will be prompt to enter her pin. A check against the database will made to check the validity.

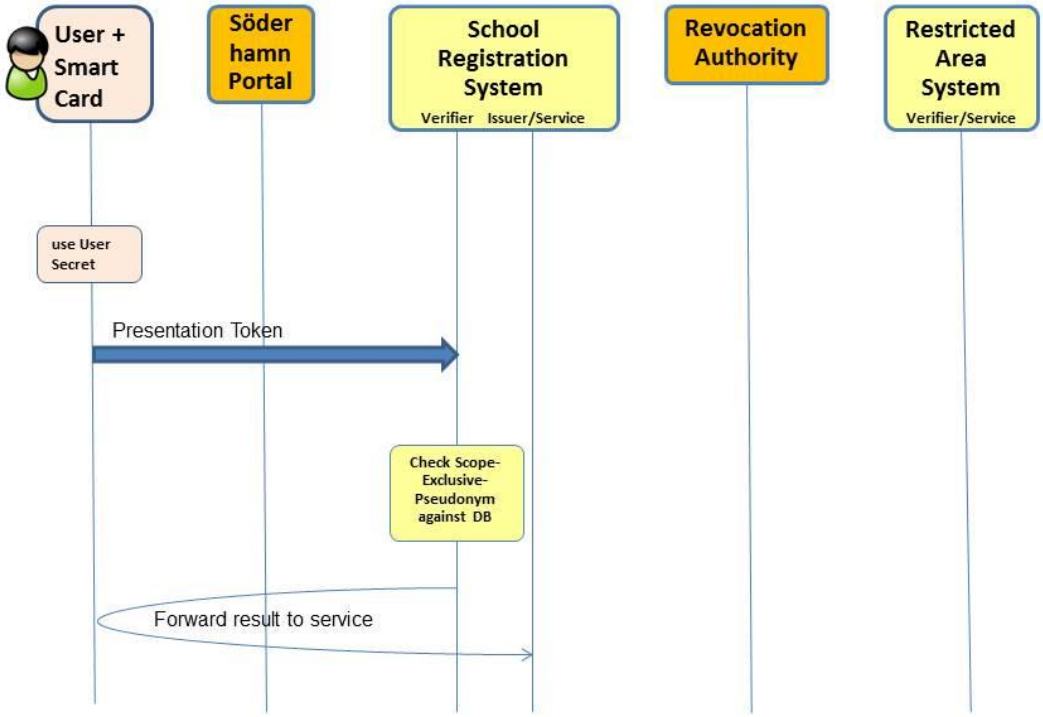

Figure 5: Login to School Registration System via ABC Technology (b)

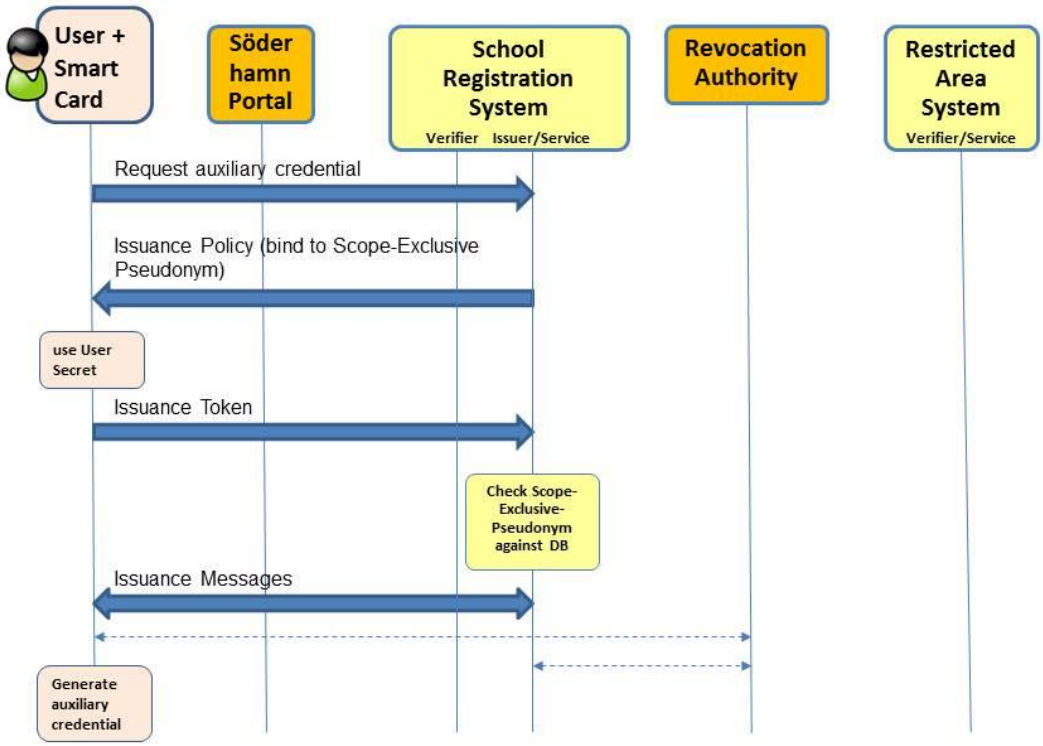

Figure 6: Obtaining auxiliary Credentials after successful Login

3.5.2 Viewing User's Attributes

Using the School Registration System the user can view her attributes that are stored in the IdM Database.

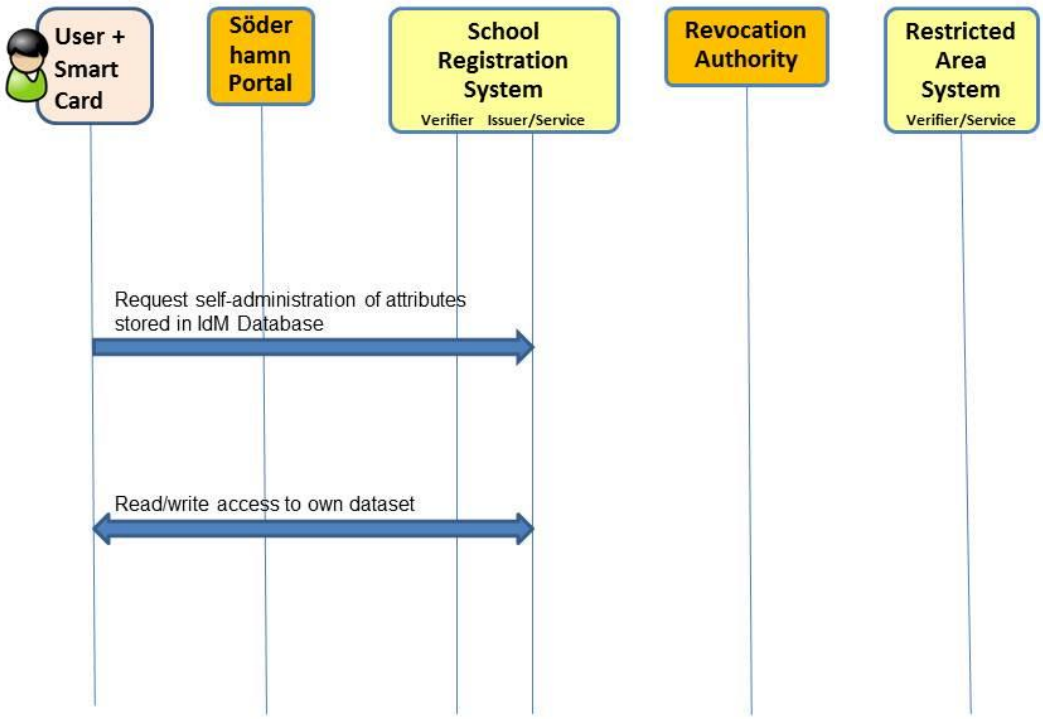

Figure 7: Viewing Attributes stored in IdM DB after successful Login

3.5.3 Inspection

If school personnel, a guardian, a pupil or law enforcement need to trace a specific user and reveal attributes that were originally hidden from the Restricted Area System they can initiate an inspection request. The School Inspector Board then decides when or if to reveal the users identity as shown in Figure 8.

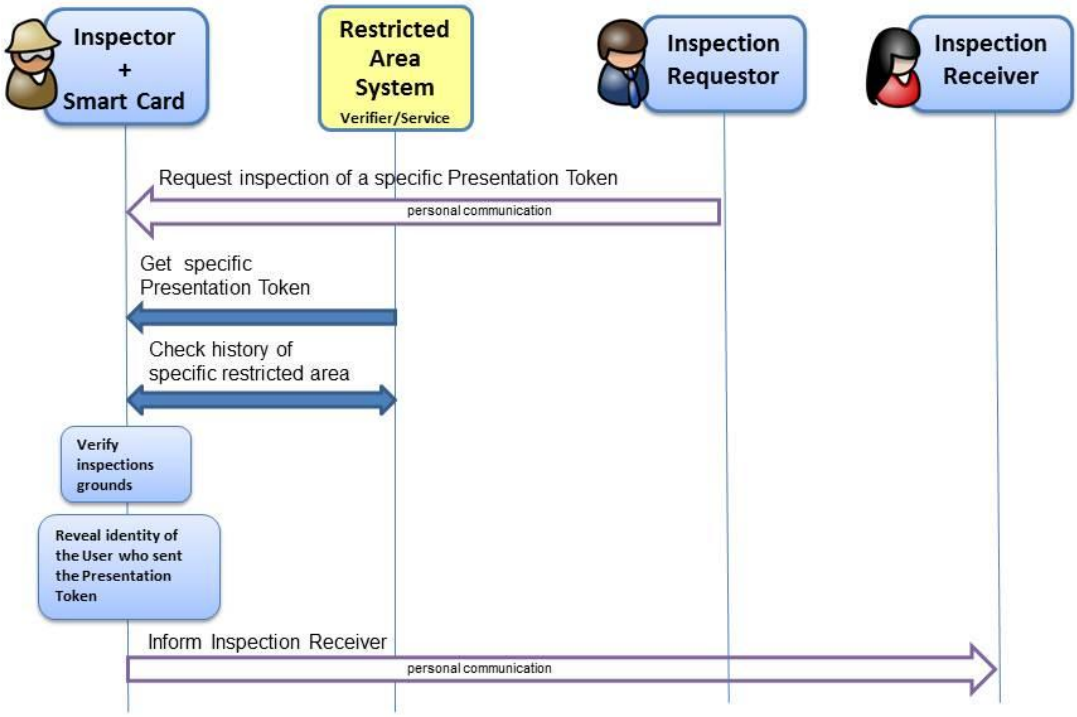

Figure 8: Inspection

3.5.4 Restricted Area

When a user wishes to visit a Restricted Area she will be redirected from within the Söderhamn Portal. A request entry will be sent to the Restricted Area System. The user may be granted or denied access based on the conditions set within the policy as shown in Figure 9 and Figure 10.

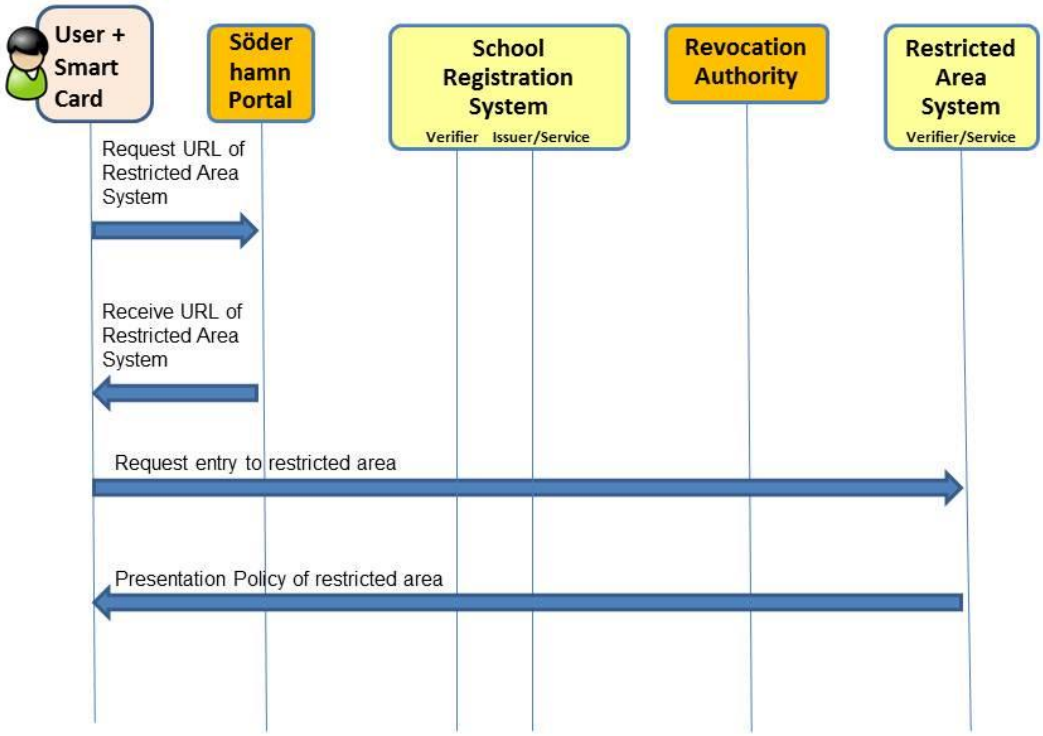

Figure 9: Restricted Area (a)

The Restricted Area System will store the presentation token retrieved from the user as shown in Figure 10.

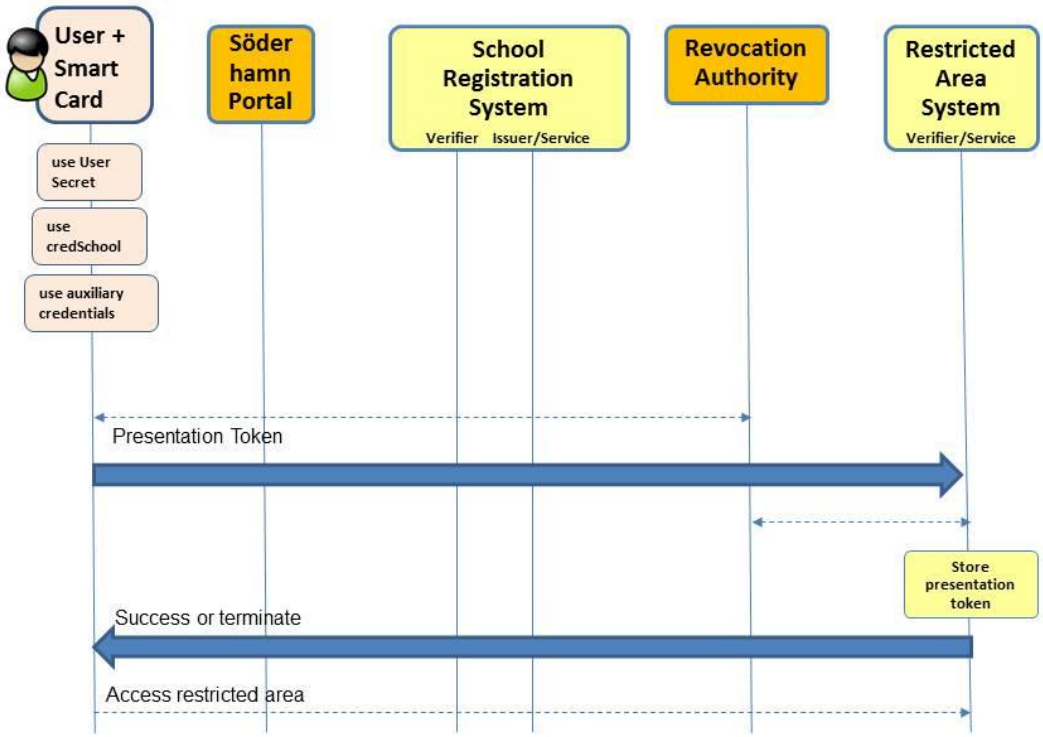

Figure 10: Restricted Area (b)

3.6 Role Mapping

To further describe and analyse the pilot and its functionality, it is necessary to map the ABC roles as they have been introduced in chapter 2 above to the acting entities in the pilot. This will be done in section 3.6.1. Likewise, this will be done for the legal roles as basis for further legal assessment in section 3.6.2.

3.6.1 Mapping of ABC roles

In the table below the roles are mapped according to the above ABC architecture figure.

Entity	ABC Role
School Administration Office	Issuer
School Personnel, Guardian, Pupil	Revocation Requestor
School Administration Office	Revocation Authority
Restricted area System	Verifier
School Personnel, Guardian, Pupil	User

Client Software	User Agent
School Inspection Board	Inspector
School Personnel, Guardian, Pupil, Law enforcement	Inspection Requestor
School Inspection Board, Law enforcement	Inspection Receiver

Below we give a detailed description of the mapped entities according ABC architecture:

Issuer: The ABC role Issuer defines the system component which issues Privacy-ABCs containing attributes to users. To be able to participate and access the system in any way the user must first interact with this system component and collect valid Privacy-ABCs so the user can prove that he/she has proper access to the system.

In order to issue credentials to users (e.g. pupil) the School Administration Office will use components (e.g. IdM) developed and administrated by NSN.

If the prerequisites for a user (e.g. pupil) should change over time the user need to interact once more with this system component and complement with new Privacy-ABCs. The School Administration Office is responsible for adding and updating information about the users in IdM provided by NSN.

Revocation Requestor: In this pilot any user (i.e. pupil, guardian and school personnel) can request for the revocation of a credential by contacting the school administration office that can revoke a pupil's credential. The school administration office will also act as a revocation requestor under certain circumstance e.g. when the pupil has unsubscribed from the school or has changed class.

Revocation reasons can be categorized in three main categories: card related, content related and behaviour related.

Revocation is mainly performed for reasons related to the smart card such as if the card is lost, stolen, corrupted, damaged or for any other reason non-functional anymore. Content, or attribute related reasons are when the content of the credential is changed e.g. if the user no longer belongs to a certain class or no longer studies a certain subject, begins studying a new subject or maybe no longer belongs to the school. Revocation may also be conducted if the user misbehaves or if the user for any reason is no longer eligible to have the credential and to use a Privacy-ABC.

Revocation Authority: A Revocation Authority is an entity that is responsible for revoking issued Privacy-ABCs upon request of the Revocation Requestor. When a Privacy-ABC is revoked, it can no longer be used for generating presentation tokens. The Revocation Requestor will be the School Administration Office which will present to the Revocation Authority a formal request with a suitable justification of the revocation request.

Verifier: The ABC role Verifier defines the system component that protects the access to a resource or a service. By presenting a policy to Users, it imposes restrictions on the credentials they must own and the information from these credentials that they have to reveal in order to access the service. The Verifier accepts credentials from Issuers that she trusts.

In the Swedish scenarios the component that acts as a Verifier is the Restricted area System. This component will interact with other components (e.g. IdM) developed and administrated by NSN to grant access to those Users (i.e. pupils) that satisfy certain properties. The Issuers that this Verifier trusts are School Administration Office.

User: The role User defines the human entity that collects Privacy-ABCs from an Issuer and wants to access a resource controlled by a Verifier. When interacting with an Issuer a User takes the role of Credential Receiver and when she desires to access a resource through a Verifier, she acts as a Prover.

The Users in the Söderhamn pilot are pupils, guardians and school personnel that will participate in the trial. In order to interact with the pilot's Issuer and Verifier, the users are represented by a software component called User Agent. This software component runs locally on their PCs and enables them to use and browse the Privacy-ABCs stored on their smart cards.

User Agent: This is an embedded software component that represents the human User and manages her credentials.

Inspector: The Inspector reveals the identity or other encrypted attribute values of a User (e.g. lifting anonymity) upon legitimate request of the Inspection Requestor. For this, the Inspector has to examine the legitimacy according to the inspection grounds. Inspection requires that at least two persons or more act jointly (e.g. principal and data protection office). This is called The School Inspection Board.

Inspection Requestor: Entity requesting an inspection from the Inspector, asserting that inspection is compliant with the inspection grounds specified or is legally required. While pupils may trigger the inspection process (e.g. in case of mobbing or threats) they are not generally entitled to gain access to the information revealed. The definition of the inspection grounds should for such cases allow the choice of appropriate reactions e.g. the choice of an inspection receiver. In case of mobbing the information might best be provided to some student elected trustworthy teacher fur dispute resolution.

Inspection Receiver: The entity receiving the reply of the Inspection. This may be another entity than the one requesting (triggering) the inspection.

3.6.2 Mapping of legal roles

The following sections will describe the mapping of legal roles as these are described within privacy legislation for the Söderhamn use case. The mapping is intentionally restricted to roles in the described in data protection rules. Besides the roles relevant data protection other legal roles may exist, e.g. the role as a class teacher bearing some responsibility over pupils or the role of a principal who is formally head of an authority and entitled to give orders or instructions to other teachers. However, as far as it can be seen by now such roles have no influence on the pilot to be set up.

3.6.2.1 Necessity of the mapping of legal roles

As a basis for further legal assessment and the evaluation of the privacy compliance, the acting entities are described below and assigned to a legal role as defined in the European data protection legislation forming the basis of the used definitions. The applicable Swedish[5] data protection legislation contains identical definitions and will be referenced in parallel. The mapping of legal roles can be understood as assigning the responsibilities foreseen in the law to an entity. These responsibilities include in particular the implementation of appropriate technical an organisational measures to protect personal data, Art. 17 Para. 1 of Directive 95/46/EC, granting the data subjects rights and to bear potential liability for the case of damages suffered due to unlawful processing, Art. 23 of Directive 95/46/EC ([Art29WP169] p. 4).[6] The decision which entity is the responsible data controller further determines which national data protection legislation is applicable, Article 4 para. 1 (a) of the Directive 95/46/EC (see [Art29WP169] p. 7); Section 4 of the Swedish Personal Data Act (1998:204).

While it is possible for the ABC roles to assign them to parts of the infrastructure (e.g. the user client) or a piece of software or process (running IdM software), legal roles must be assigned to a natural or legal person[7]. Due to the nature and purpose of the legal roles to assign rights and obligations only

[5] English translations of the Swedish "Personal Data Act (1991:204)" and the Personal Data Ordinance (1998:1191)" are available online: http://www.datainspektionen.se/lagar-och-regler/patientdatalagen/

[6] See also Recital 25 of Directive 95/46/EC.

[7] Legal persons are non-human entities to which the legal system has granted personhood thus to bear rights, privileges, duties, responsibilities and liabilities under the law, e.g. registered corporations or parts of states such as federal states, regions or municipalities.

those entities can be understood as an entity in the sense of the directive that can bear rights and duties under the law.[8] This is clearly stipulated in Art. 2 Para. 2 (d) of Directive 95/46/EC:

> "(d) 'controller' shall mean the **natural or legal person, public authority, agency or any other body** which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for her nomination may be designated by national or Community law;" (emphasis added)

For the Söderhamn use case this will mean that the responsible legal entities need to be identified. Such entities may include schools, local authorities, or government departments ([Car09], p. 23). Which entities are accepted as legal entities with the possibility to bear rights and duties is governed by the national law of the country of incorporation.[9]

For the pilot in Söderhamn the acting entities with legal capacity are:

- Eurodocs – the project Partner of ABC4Trust is providing the infrastructure including hard- and software to use Privacy-ABCs.
- Söderhamn Kommun is the legal entity bearing rights and duties of the secondary school "Norrtullskolan". In the following references to the school, school administration or Norrtullskolan legally mean the school legally represented by Söderhamn Kommun.
- Nokia Siemens Networks (NSN) – The project partner NSN operates the Identity Management system. At the current state of planning it will provide this service for the Söderhamn pilot, e.g. by providing and setting up the infrastructure and providing ongoing support via telephone or remote maintenance of the system.
- Participants: pupils, students, teachers, and other staff of the school are natural persons that participate in the pilot trail. All natural persons are endowed with legal rights and are therefore relevant entities for the pilot.
- Selected trustworthy persons: For the Söderhamn pilot some selected persons will take the role as Inspector holding the secret key to decrypt identity information contained in presentation tokens. By the time of the editorial deadline of this deliverable it has not been finally decided which persons will take the role of an Inspector.

3.6.2.2 Legal roles to be assigned

For an overview and definition of the legal roles see the chapter "Definition of roles" above (see Chapter 2 above). Among the roles defined within data protection law (data controller, data processor, and data subject) the entities acting may take different roles depending on the current type of processing undergone. In particular the role of data controller can be assumed by several entities for a single processing operation. This type of joint controllership is explicitly mentioned in Art. 2 (d) of

[8] But see [JCBHWZ09] where the idea of virtual persons is proposed. A virtual person is any entity that can have rights and duties. Such rights may include access rights and thus also systems, software agents, or processes can be understood as virtual person. While this can be seen as underlying idea for mapping ABC roles to non-human entities this approach does not provide further insight for the mapping of legal roles, rights and obligations as the current law so far only accredits natural and legal persons to bear rights and duties in the sense of the law.

[9] For the area of legal entities founded under private law see European Court of Justice, stating that the recognition of foreign companies founded in other EU member states is a necessary precondition for the freedom of establishment, European Court of Justice, Judgement of the court, November 5th, 2002, Case C-208/00 – Überseering, Para. 59, online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000CJ0208:EN:PDF

Directive 95/46/EC and Section 3 of the Swedish Personal Data Act (1998:204). For joint controllership it is not necessary that the partners have equal influence but any form of processing together or "not alone" suffices for joint controllership ([Art29WP169] p. 18). Identifying the legal roles requires an overview of the planned services and setup of the pilot naming the involved parties:

The Restricted Area System is set up and operated by ABC4Trust partner Eurodocs, to provide social network functionalities to the school for direct, anonymous or pseudonymous communication among pupils, teachers, and parents. Based on an authentication with Privacy-ABCs, the system allows instantiating and accessing restricted areas. Such a restricted area may contain forums, chats, polls or may be used to share files. The content and structure of a restricted area is determined by the User instantiating the restricted area. Some restricted areas will be predefined by the system, e.g. those for all students of a particular class, for a project and for counselling. The intended purpose of the system is to provide social network functionalities for the communication among pupils and school staff.

Generally, the system can be seen as a social network as it provides comparable functionalities. For social networks in a broader sense and some particular commercial ones analysis of the legal roles exist already ([Art29WP163]; [KuLeBe10]; [KarTho11]). The provider of a social network can be seen as responsible data controller as the provider makes the means for processing personal data and 'Basic' services such as the user management available ([Art29WP163], p. 5; [KuLeBe10], differentiating). Besides the provider also the User instantiating a restricted area may be a data controller in particular if she publishes personal data of third parties such as pictures or names of others (cf. [KarTho11], p. 18; [JaRo11], p. 161).

In consequence joint controllership is given in the Söderhamn pilot between the school and Eurodocs. Both entities are operating the system and different components with the aim to provide social network services to the students and to deploy the possibilities for communication in daily school routine. While Eurodocs provides the soft- and hardware as well as several basic services (forum, chat) the school acts as the identity service provider issuing credentials and also regulating access to the predefined and other Restricted Areas set up by school personnel.

Besides the provider and the school also the User publishing information within a Restricted Area may become a data controller, if she publishes personal data of other persons. In contrast to facebook (see [FAC04]) and other commercial social networks the Söderhamn pilot will neither transfer this information to countries outside of the area of application of Directive 95/46/EC nor will Eurodocs claim rights on the content provided or track and profile the Users. In these cases the Restricted Area system merely serves as a platform for the communication between individuals. With these essential differences in mind it appears acceptable to extend the so called household exemption for data processing of purely private nature (see Art. 3 sec. 2 of Directive 95/46/EC and Sec. 6 of the Swedish Personal Data Act (1998:204)) to restricted areas with only identified persons communicating with each other. However, for Restricted Areas that are not restricted to a set of specific persons but rather to a group of persons sharing the same attributes the Users remain joint data controllers with Eurodocs.

3.6.2.3 Mapping of legal roles to the acting entities

The following analysis is done under the assumption that Users in the Söderhamn pilot are not identifiable with other means. According to current planning the server running the restricted area system will not protocol IP addresses of Users or set cookies to track their behaviour. The participants will in addition be informed about this potential way to identify a User and profile interests via IP addresses. Countermeasures against this type of tracking e.g. by deploying proxy services or onion routing for anonymity, may be briefly explained in an age respecting manner as part of the educational aspect of ABC4Trust. However, the problem that Users can be identified or tracked via these channels is not object of the ABC4Trust project. The underlying problem can be considered solved with available technologies such as onion routing. Consequently it is only treated as a side issue in the following description and only addressed where necessary.

As the pilots are still under development and the assignment of task to entities may be modified, some of the legal evaluations may change until the launch of the pilot or throughout the projects duration. An update will be provided with a later deliverable within this work package. For the Söderhamn pilot, the legal roles can be currently mapped as shown in Table 3 below.

Entity	**legal role**	**comment**
School Administration acting as normal administration of the school	Data controller	Processing for own (legally assigned) purposes of the school such as student registration, keeping records on attendance and scholastic performance. The school determines the means and purpose of the processing and is a data controller.
School Administration adding User's data to the database of the IdM application	Data controller	If the school administration provides excerpts of the student database for the purpose of performing the ABC4Trust pilot this is a change of purposes requiring a own legal ground for the processing. For the pilot this can be a freely given informed consent. The IdM database will not be operated under full control of the school but is physically located under with Eurodocs. In regard to the participant data Eurodocs will not assume control over the data but process these on behalf of the school being bound to the schools instructions regarding this data. Eurodocs will act in this relation as a data processor
School Administration running the IdM Portal	Data controller	The school acts as entity operating the IdM Portal and providing a method to enforce the data subject's right to access and rectification of personal data. The school controls the means and purposes of this type of processing and therefore is a data controller in this respect. Eurodocs acts as data processor on behalf of the school.
School Administration running the IdM Application	Data controller	The school an entity operating the IdM Application and is a data controller.
School Administration running the ABC system (issuing credentials, etc)	No role	No particular role for this task as it is just an aspect of being data controller of the personal data of the pupils and staff in the schools IdM system. The school plans to make the identity information useable for the data subjects by acting as a credential provider. For this issuing credentials and verifying claims are efforts to implement technical and organisational measures for ensuring data security by enabling usage

Entity	legal role	comment
		of unlinkable and privacy enhancing Attribute-based credentials. In addition, the IdM portal also provides transparency in the privacy sense as it enforces the right of access to the database and allows rectification for selected entries.
Eurodocs and the school running the Söderhamn portal and administering restricted areas.	Joint controller	Both Eurodocs and the school determine the purpose of the system which is to allow pupils to use the services (similar to social network services) provided by the system that will be set up during the pilot. Eurodocs is directly influencing the system by providing the hardware and software and with design decisions regarding the whole pilot. Therefore Eurodocs is a data controller in this setup, too. The school, represented by the teacher of person that will be responsible to administer restricted areas, is also a data controller of the personal data processed. The school here determines the use of the system by providing specific restricted areas and by including them into the school's routine. However, the parties are not data controllers if the data processed is not person related. This is the case if the data cannot be linked to an individual, e.g. if posting into a forum was made using a credential that does not allow such linking.
Eurodocs running the IdM public directory	No role or data controller	The IdM public directory will contain a repository for public keys of servers, inspectors and components of the ABC infrastructure. At the current state of planning this server will not process personal information. Depending later decisions it may become necessary to identify the inspectors by name. In this case processing and distributing their certificate including their name and position would constitute processing of personal data. Eurodocs would then be a data controller in this case determining the use of the information within the pilot.
Users (pupils, parents, school personnel) obtaining credSchool	Data subject	Participants obtaining a credential are data subjects if the entity issuing the credential processes personal data. The school credential contains personal data such as

Entity	legal role	comment
		name and Civic Registration Number[10]. Likewise the guardian credentials and child credentials contain personal data.
Users (pupils, parents, school personnel) obtaining further credentials such as credRole	Data subject	Obtaining additional credentials usually requires that the user identifies herself. She is therefore a data subject in relation to the Issuer.
Users (pupils, parents, school personnel) using further credentials such as credRole	Data subject if identifiable	If the attribute values of the credential (e.g., the roles in credRole) allow linking to a User, this User is a data subject. This could be the case for small anonymity sets as could happen for groups with few registered members such as school principals, counsellors, coaches. If the anonymity set (cf. [PfiHan10], p. 9)is large enough the User of the credential is anonymous and not identifiable and therefore not a data subject due to using the credRole.
NSN as operator of the IdM portal and IdM database	Data processor	Maintenance and service for the IdM system makes remote access necessary for ABC4Tust partner NSN who provides the necessary IdM infrastructure. The infrastructure will be set up in Sweden on Eurodocs premises. Administrative rights to the IdM system include at the current stage a possibility to access the personal data of the students. NSN will operate as a data controller for the school administration.
Users viewing or administering their personal data in School System.	Data subject	Users who make use of their data subject's right to obtain from a controller access their personal data according to Art. 12 (a) of Directive 95/46/EC or Section 26 of the Swedish Personal Data Act (1998:204) are data subjects. Users who make use of their data subject's right to rectify incomplete or inaccurate personal data according to Art. 12 (b) of Directive 95/46/EC or and Section 28 of the Swedish Personal Data Act (1998:204) accordingly are data subjects.

[10] The Swedish personal identity number was introduced in 1947 and is assigned to all residents and widely used in public areas such as education (schools, universities), social security, but also for private sectors such as banking.

Entity	legal role	comment
Eurodocs providing the Restricted Area System	Data controller	Eurodocs controls the system and decides about the means of data processing. It also determines the general purpose of the system to enable communication among the participants. Even though most contents and accesses of pupils will be anonymous some interactions will contain personal data. At least the tokens containing the inspection information will also be processed by the Restricted Area system and must be regarded personal data even if the information is encrypted. See the text preceding this table on this question.
Entity anonymously instantiating and operating a restricted area that can be used anonymously	No role, directive not applicable	No role. In the sense of the Data Protection Directive here no identifiable person or the respective data of such a person is concerned.
User anonymously accessing and using a 'Restricted Area'	No role	Data subject in regard to own personal data used for authentication. A User is anonymous if the anonymity set ([PfiHan10], p. 9) is large enough to prevent an identification of the User within the set of users. For certain combinations of attributes the set might be so small that identification becomes possible (e.g. only girl aprticipating in the drama group and the school's chess team). If the Usser is not identifiable the data protection directive is not applicable. Without being identifiable the User is in consequence not a data subject and does not have the data subject's rights of access or rectification (so for the German BDSG Dammann in [Sim11] § 3 BDSG para. 36).
User publishing personal data of a third person in a restricted area.	Data controller	Users publishing personal data of other persons in a social network determine the means and purpose of the processing and are therefore data controllers. The so called household exemption for purely personal and household activities does not apply for cases in which data of third parties is made available in social networks [Art29WP163]. As at least the social network provider gains access to this information the User is responsible data controller in these cases.
Entity instantiating and operating an restricted area	No role	A User instantiating a restricted area does not gain access to the presentation tokens

Entity	legal role	comment
with inspection enabled		including the encrypted inspection information. These are provided towards and verified by the Restricted Area System. Instead, the User only learns that another party joining these areas fulfils the set requirements. However, the entity operating the Restricted Area System (Eurodocs) is data controller as the inspection information contains the personal data – even if it cannot be decrypted without aid from the Inspector (cf. [Art.29WP136], p. 16 et seq.).
Entity retaining presentation tokens with inspection information (here Eurodocs operating the Restricted Area System)	Data controller	The fact that personal data is not visible to the entity operating the Restricted Area system does not negate the property of the data being personal. It is sufficient that someone (here: the Inspector) can identify the data subject by decrypting the information.[11]
User anonymously accessing a 'Restricted Area' with inspection enabled	Data subject	With the Inspection token the Restricted Area System receives and processes (encrypted) personal data identifying the User. The User is identifiable by the Inspector who can decrypt the information provided for inspection (cf. [Art.29WP136], p. 16 et seq.).
Counselling: pupil accessing a Restricted area dedicated for counselling (inspection enabled)	Data subject	In relation to the operator of the Restricted Area System the User is a data subject as she can be identified with aid of the Inspector (see above). The counsellor is generally not able to identify the User. However, the counsellor may request an inspection if the inspection grounds are met. If the counsellor is subject to professional secrecy it may even be that she must be part of the inspection process as only the bearer of the professional secrecy may decide about revealing the identity of clients or patients. To this end the pilot requires further

[11] This expansive understanding of what identifiable person directly influences the scope of personal data in the sense of Art. 2 sec. (a) of Directive 95/46/EC. The view supported by Recital 26 of Directive 95/46/EC which states "... whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person;...". However, due to the implication of massively broadening the scope of the Directive this issue has been object of an ongoing legal debate in particular in relation to dynamic IP addresses and cookies. The European Court of Justice recently stated that IP addresses are personal data (see Judgment of the Court 24 November 2011 - Case C-70/10 - Scarlet Extended, para. 51). Similarly the Article 29 Working Party already stated that IP-addresses ([Art29WP136] p. 16) and cookies ([Art.29WP148] p. 9) are person related data. For an objecting legal view and a detailed display of the ongoing legal debate in Germany with further references see e.g. [KrüMau11].

Entity	legal role	comment
		planning.
Counselling: person of the counsellor (anonymously)	Data subject	Counsellors will be personally identified so that pupils know to whom they communicate. Taking this role counsellors are data subjects.
School Administration sharing documents (exam results, grades, etc.)	Data controller	The school administration is data controller for these data, as the processing of this information is essential part of the tasks assigned to the school. The school is obliged to ensure data security also when deploying external data processors.
Pupils sharing documents under their identity (e.g. homework or any contribution which is identified with a name within collaborative workspaces)	Data subject	These users are identifiable and therefore are data subjects.
School Administrator revoking a User's credential	Data controller	Administrator needs the User's identity to revoke a particular credential.
Inspector holding secret key that allows decryption of inspection information in presentation tokens	No role	The data identifying a person is contained in the presentation token which resides with the Restricted Area system and is not under control of the Inspector.
Inspector holding secret key that allows decryption of inspection information in presentation tokens once she receives a token for decryption	Data controller, receiver	Once the Inspector gains access to a presentation token with personal information encrypted inside, the Inspector is a data controller. Besides the decrypted identity information the inspector will usually learn about the content of the restricted area in question as this will often be necessary to decide about the plausibility of the inspection request (unless e.g. a court warrant has anticipated the decision of the inspector).
Inspector doing necessary protocol and documentation of inspection requests	Data controller	The Inspector (or better the obligations resulting from the declarations in the inspection grounds) determines means and purpose of the processing in regard to the person or entity making the inspection request and the entity who's personal data are revealed by the inspection process.
Entity receiving inspection results	Receiver	Any entity – internal or third party – receiving the information revealed by the inspector is a receiver. Exception: Authorities which may receive data in the framework of a particular inquiry are not receivers according to Art. 2 (g) of Directive 95/46/EC.
Revocation Authority	Data controller	Usually the Revocation Authority acts only on a justified request from an entitled Revocation Requestor. It will be possible

Entity	legal role	comment
		for the Revocation Authority to identify the Requestor and the User whose credential is to be revoked.

Table 3: Matching of legal roles

3.6.2.4 Further legal responsibilities

The above analysis does not cover other responsibilities outside of the area of data protection law in a broad sense. If the data processes is not personal data as it cannot be linked to a specific person Directive 95/46/EC is not applicable. However, national law may provide further protection and processing of such data may interfere with Article 8 of the European Convention on Human Rights. Besides these other areas of (national) law may be at stake such as criminal law (e.g. for defamation), tort law or anti-discrimination law [Art.29WP136].

4 Patras: Course Rating by Certified Students

In this chapter an overview of the Course Rating by certified students pilot is provided. Initially the high level components of University pilot Architecture are described. A mapping of the presented legal and ABC roles is adapted to the University pilot's Architecture. Based on the presented Architecture the University pilot's set up phase and usage scenarios that describe the general functionality of the system from the users' perspectives are defined. The last section concerns the need, usage and format of credentials.

4.1 Architecture

The general architecture of the ABC4Trust pilot as it will be deployed in Patras is depicted in Figure 11 below and further described within this section.

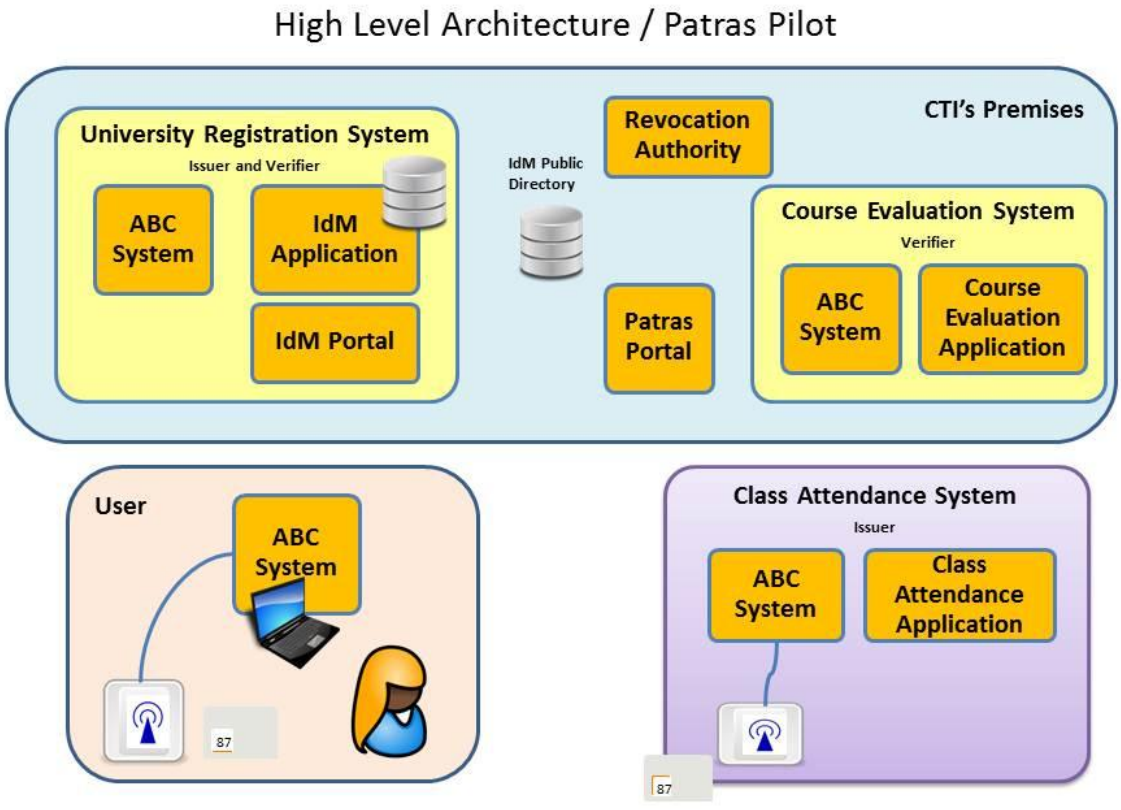

Figure 11: High Level Architecture of the Patras Pilot

As can be seen from the previous figure, the architecture of the Patras pilot is based on various components. These components have different functionalities and roles based on the scenario and use case definition of this pilot. Next, we describe the functionality and the characteristics of each high level component that is presented on the architecture figure. Note that the user interactions with the

Patras Portal, University Registration System and Course Evaluation System are online whereas her interactions with the Class Attendance System are offline

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

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

- CTI with collaboration of a university registration office employee has the possibility to insert to the database of the University Registration System the personal information of the student-volunteers that will participate in the pilot. This activity does not require ABC technology.
- A university registration office employee can make a request to the revocation authority in order to revoke a student credential. This may happen when, for example, a student graduates from the university or upon student request (smart card loss).
- Students can collect credentials that certify that they are valid students of the University of Patras
- Students are able to browse their personal data that is stored in the IdM database
- Students are able to administrate some of their personal data (e.g. course)
- Students can collect credentials that certify that they have registered to a course

When the IdM application is required to issue Privacy-ABCs to users (e.g. university credentials, course credentials – see scenario 4.3.1) it invokes the ABC System which is responsible for performing the issuing protocols. When a user wants to browse her personal information, the IdM application uses the IdM portal that supports this functionality.

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

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

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

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

- Course professors have the possibility to upload questionnaires regarding their course and determine the threshold number of attended lectures required for participating in the evaluation. This activity does not require ABC technology.

- Students are able to evaluate courses that they have registered to and attended
- When the evaluation procedure is completed, CTI members will collect and process the evaluation results in order to provide accumulated course evaluation results to HQAA. This off-line activity does not require ABC technology.

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

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

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

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

4.2 ABC System Setup

This section describes the ABC System Setup. That is, it provides a high level description of the procedure through which the user secrets of all the ABC users, as well as the issuance keys and the issuers' parameters (containing their public keys) of all ABC issuers are generated.

The ABC System Setup is triggered by two main events which are described below:

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

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

At this point, each system administrator does the following:

He starts a script to generate the issuer parameters and the issuance keys for the issuers she is responsible for. In particular, this is done for the University Registration System and the Class Attendance System.

The issuer parameters of the University Registration System are stored on the IdM public Directory and can be accessed by the ABC systems.

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

4.3 Scenarios

It is necessary the University pilot's Architecture to be able to coexist or be interchanged across scenarios involving all users and pilot's application systems. Based on the presented Architecture we have defined the University pilot's usage scenarios that describe the general functionality of the system from the users' perspectives. We use the following basic scenarios that provide step-by-step descriptions of how the proposed system architecture should operate and interact with its users under a given set of circumstances.

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

4.3.1 Obtaining the University/Course Registration Credential

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

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

4.3.2 Obtaining Class Attendance Data

All the students that will take part in the evaluation of two courses have to prove their attendance for a sufficient number of lectures without, however, revealing the exact attendance ratio and which lectures she visited. This scenario uses the Class Attendance system presented in pilot's architecture in order to collect students' attendance information. Since Set up phase has finished all the students that will take part in the evaluation of two courses have been issued Privacy-ABCs that certify students' information (first name, last name, etc.) and information related with the course. Student can log on to IDM portal and can view and administrate some of her own data using these credentials.

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

4.3.3 Backup and Restore of Class Attendance Data

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

We assume that the student attended some course lectures (see obtaining class attendance scenario) and has some attendance information stored on her smartcard. Student could run locally User Agent application on her PC in order to browse the Privacy-ABCs stored on her smart card, delete credentials or backup the smart card content on her PC. In order to retrieve the attendance data, the User Agent application prompts student to enter her PIN. Student should connect her smart card reader to her PC before starting user agent application. The backup data must be encrypted by using user agent application for backing up, a PIN is required to unlock the card and store the data on the PC.

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

4.3.4 Revoking a Student's Privacy-ABCs

In some cases the University registration office has to be able to revoke a student's credential. As a first example, when a student has lost her smart card, she must declare her smart card lost to the University Registration Office where she can get a new envelope (containing PIN, PUK) and a smart card. The University Registration System Administrator revokes the student University credential and deletes the scope-exclusive-pseudonym from the ABC system. Then the student has to obtain a valid student and course credential and she will be able to use the backup data from her PC (see Scenario 4.3.1 and 4.3.3).

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 scope-exclusive-pseudonym from the ABC system.

4.3.5 Course Evaluation

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

This Course Evaluation 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. Each student should have an ABC4Trust SC reader and have installed the ABC user agent on her computer in order to start the course evaluation procedure. Students are able to participate anonymously in a course evaluation by logging in to the Course Evaluation System via ABC technology. Whenever a student wants to evaluate a course she can access the Patras portal though her computer and the smart card reader. Then the Patras Portal will redirect him to the course evaluation system where only users satisfying certain policies will be able to access. If the Course Evaluation System is not online or if the Course Evaluation System is not yet enabled, the student will receive a suitable notification. The student will be able to fill in the uploaded questionnaire if she satisfies the following policies:

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

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

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

4.4 Privacy-ABCs

The overall goal of the "Course Rating by Certified Students" scenario is that students can anonymously state their opinion about a course to which they are registered and sufficiently attended. While anonymity is an imperative requirement, trust is another one that has to be guaranteed. That is, only certified students i.e. students that are registered to Patras University, students that have registered to a specific course and have attended a minimum number of lectures, should be able to evaluate this course.

As already described in the scenario definition of the pilot, during its deployment a student is being issued different types of credentials. First of all, in the beginning of the trial a student should contact the University Registration System in order to collect a credential (credUniv) that guarantees that she is a student of the University of Patras. When a student desires to register to a course she collects a second credential (credCourse) through the University Registration System. Finally, when a user attends to a lecture of a course she collects a credential (credAttendance) by passing her card near the NFC reader that is located in the classroom. The contents of these types of credentials are described next.

4.4.1 credUniv

This is the type of credential that a student collects the first time she contacts the University Registration System. credUniv is bound to the User's User Secret. It certifies that the student is a valid student of the University of Patras. This credential is the electronic equivalent of the real life "student's card" and thus contains the following attributes:

- First Name
- Last Name
- University Name
- Department Name
- Matriculation Number
- Revocation Handle

The revocation handle will be used when a credential of type "credUniv" needs to be revoked, e.g. when a student graduates.

4.4.2 credCourse

This is the type of credential that a student collects from the University Registration System when she decides to register for a course. credCouse is issued from scratch and not bound to anything. This credential requires a link with the student's "credUniv" credential and that is why the matriculation number is also included as an attribute in this credential. Thus, the attributes contained in the credential of type "credCourse" are:

- Matriculation Number
- Course Identifier

4.4.3 credAttendance

This is the credential that a student collects when she attends to a specific lecture of a course. The credential issuance is performed when the student swipes her smart card on the NFC reader that is located inside the classroom. As in real life students can anonymously attend a lecture, during the issuance of "credAttendance" the NFC reader must not know any student's attributes that can be linked with her identity. This link would also prevent students from exchanging theses credentials. Thus, an issuance with advanced features is performed in order for the student's matriculation number to be *invisibly* carried over from her "credUniv" to the new "credAttendance". credAttendance is not bound to anything. The "credAttendance" type of credential contains the following attributes:

- Matriculation Number
- Course Identifier
- Lecture Identifier

4.4.4 Proofs about Credentials

Students of Computer Engineering and Informatics Department will be issued credentials that certify a number of facts about them (e.g. matriculation number, name, department, percentage of attendance of a course, etc.), allowing those with proper credentials to anonymously provide feedback on two courses and teachers they had during a semester.

To be eligible to participate in a specific course evaluation, the students must have a valid credUniv and a credCourse which must match to the course the student is currently evaluating. Each student uses both of these credentials in order to prove that they contain the same matriculation number. The students must also prove that they have attended to a sufficient number of course lectures by using the credAttendance credentials. The number of sufficient attended lectures will be provided by the Course Evaluation System in its presentation policy.

The Course Evaluation System must therefore be able to check if the User's credUniv has not been revoked and

- if the course identifier from the User's credAttendance credentials and the User's credCourse credential are the same and applicable for the current course evaluation
- if the matriculation number in all credAttendance credentials meeting the above condition are the same as the matriculation number located in credUniv and credCourse
- if all n credAttendance credentials meeting the above 2 conditions are unique (no duplicates which attest the attendance of the same lecture)
- and if the resulting number of credAttendance credentials meeting the above 3 conditions are higher than or equal to the minimum number of visited lectures defined by the Course Evaluation System.

4.5 Data Flows

In this section we give a detailed description of the basic scenarios data flows between architecture entities.

4.5.1 Obtaining the University/Course Registration Credential

When a student wants to register at the University and obtain a valid student credential, she browses the Patras portal which redirects him to the University Registration System login page. The student now can log in using the OTP provided in set up phase. Figure 12 presents the corresponding data flows.

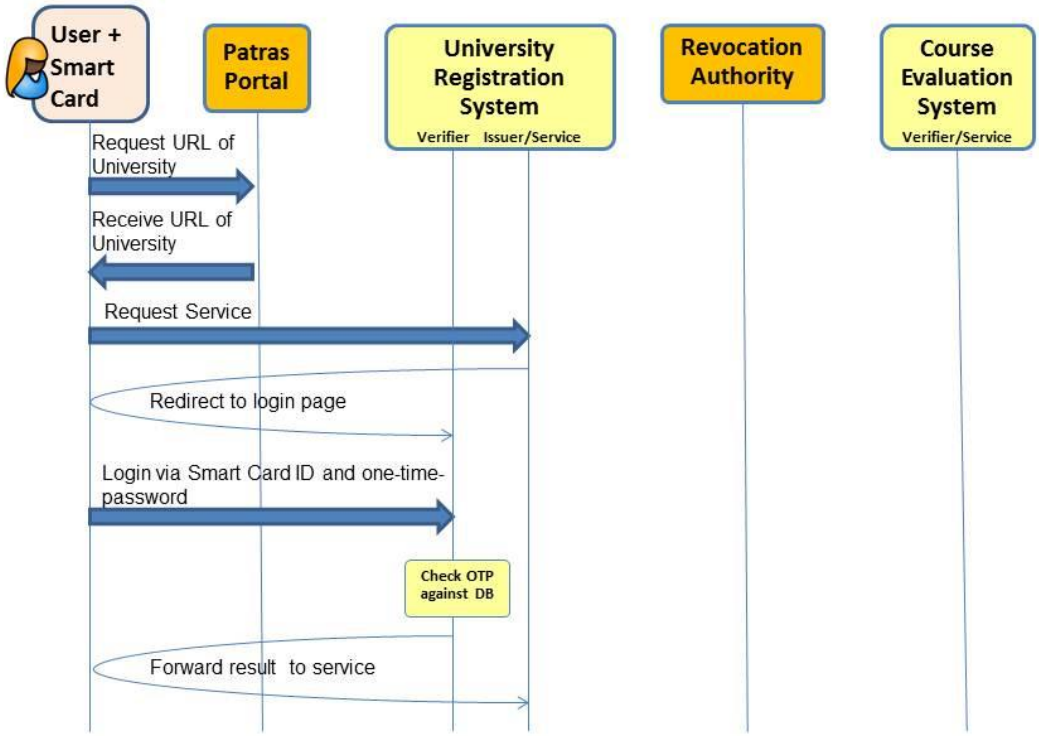

Figure 12: Bootstrap / Obtaining first Privacy-ABC (a)

At the next step, student initiates an issuance protocol and a valid student Privacy-ABC is stored on her smart card. Figure 13 gives a detailed description of the data flows needed in order to get the credUniv Privacy-ABC.

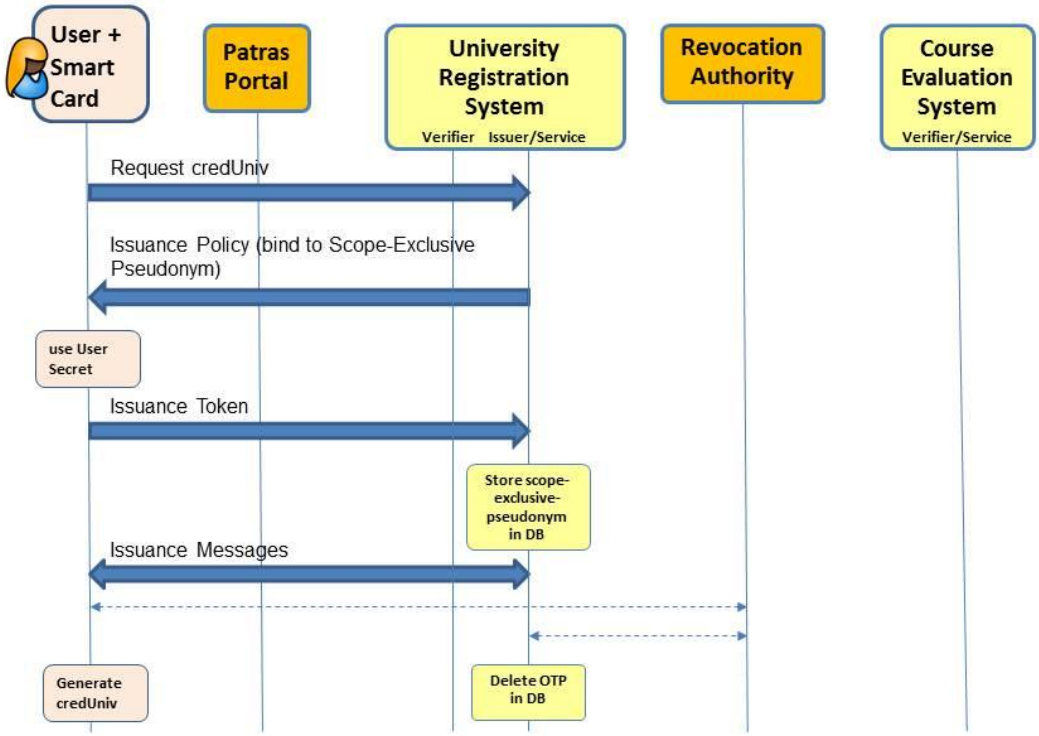

Figure 13: Bootstrap/Obtaining first Privacy-ABC (b)

When a student wants to book a course, she will first browse to the Patras portal and then will log in to the University Registration system via ABC technology. Figure 14 and Figure 15 describe the data flows needed at this phase. Finally, the data flows for obtaining a course credential are depicted on Figure 16.

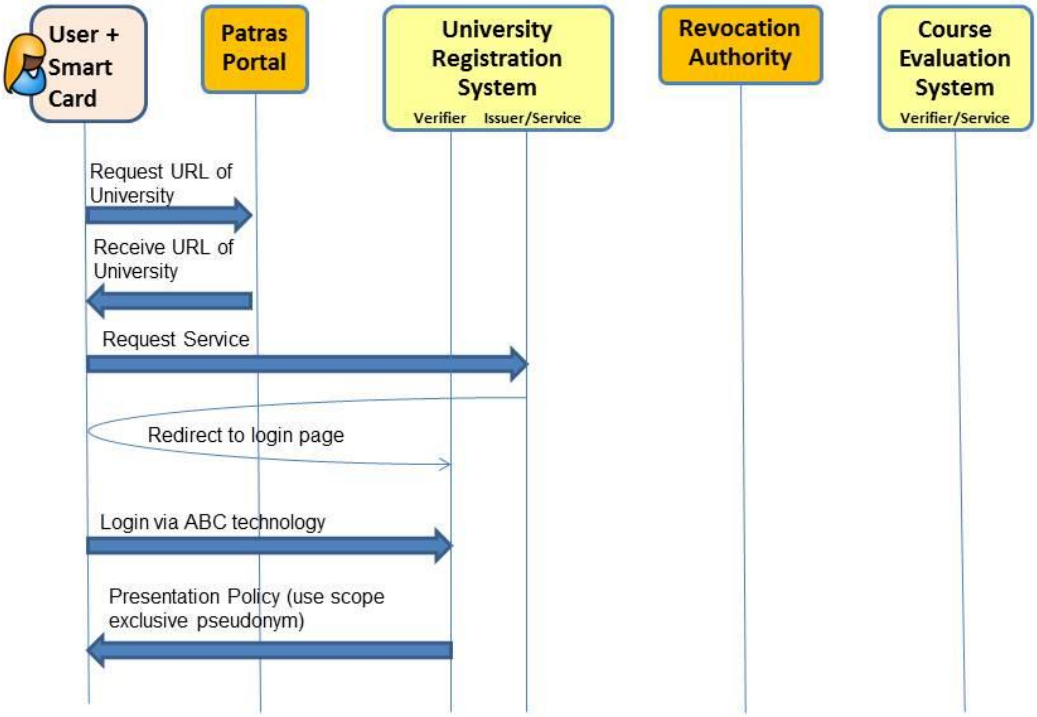

Figure 14: Login to University Registration System via ABC Technology (a)

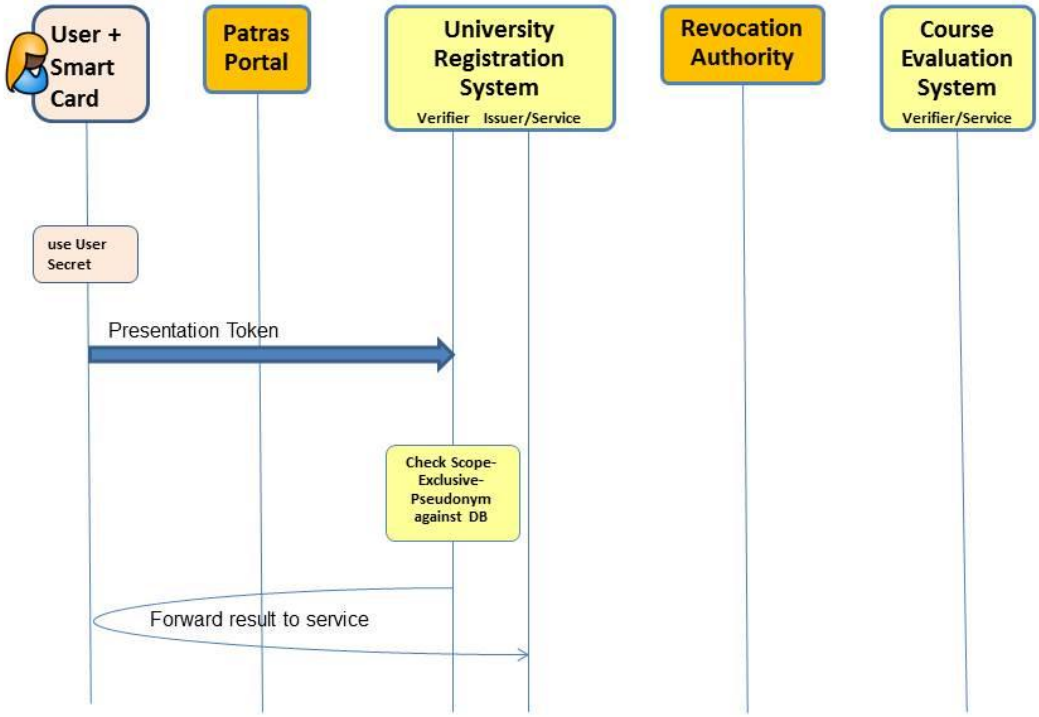

Figure 15: Login to University Registration System via ABC Technology (b)

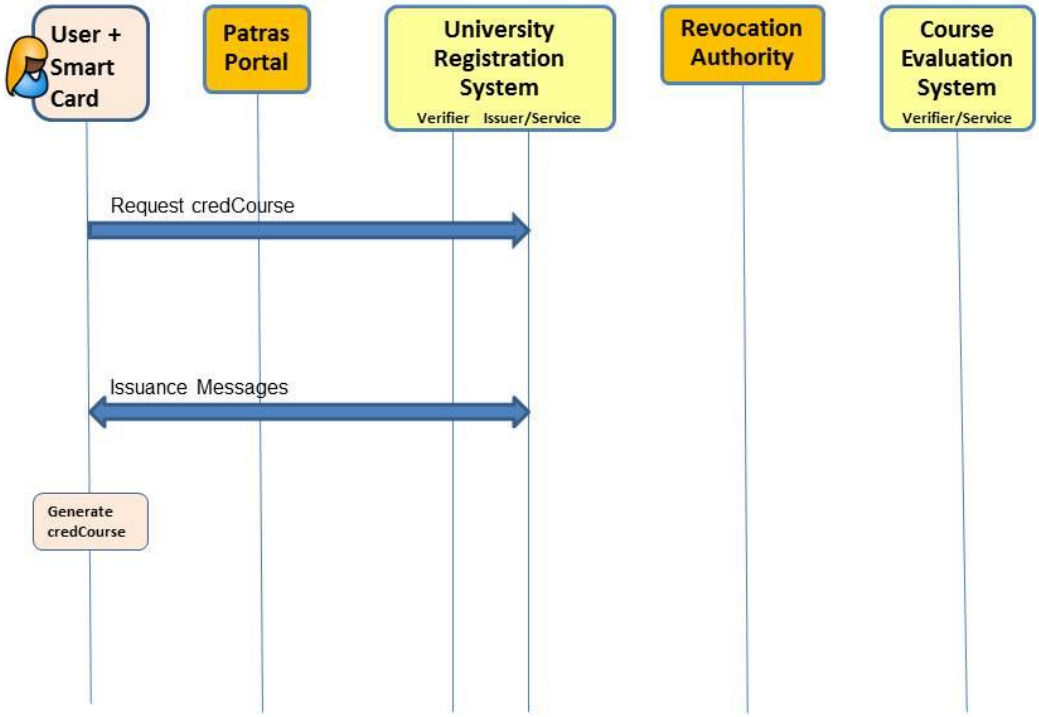

Figure 16: Obtaining credCourse after successful Login

4.5.2 Obtaining Class Attendance Data

When a student attends a course lecture, she waves her smart card on the Class Attendance System in order to collect a credAttendance Privacy-ABC. For more details about data flows see Figure 17.

bellow.

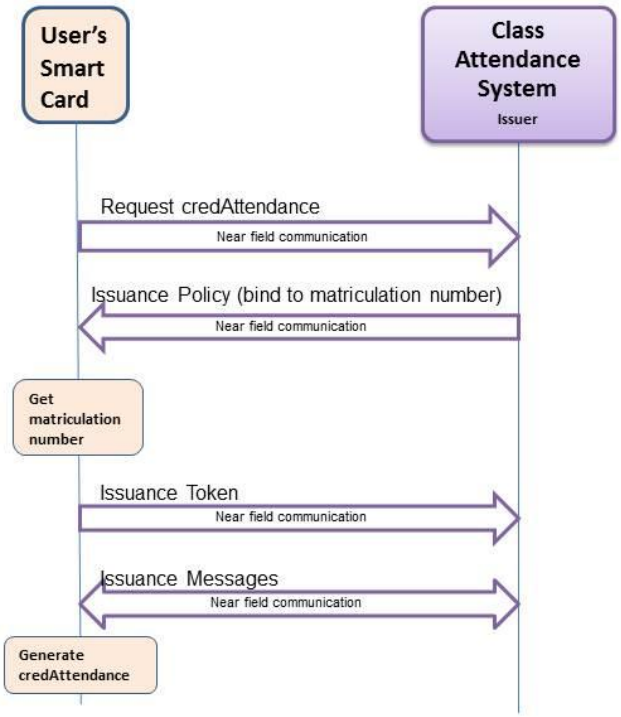

Figure 17: Obtaining credAttendance

4.5.3 Course Evaluation

Students will be able to participate anonymously in a course evaluation by logging in to the Course Evaluation System via ABC technology as seen on Figure 18. More precisely a student requests to participate in the course evaluation and Course Evaluation System replies with a presentation policy.

When a student satisfies the required policy the Course Evaluation System prompts the student to fill in the evaluation form and stores the result of the last submitted course evaluation. The corresponding data flows are seen in Figure 19.

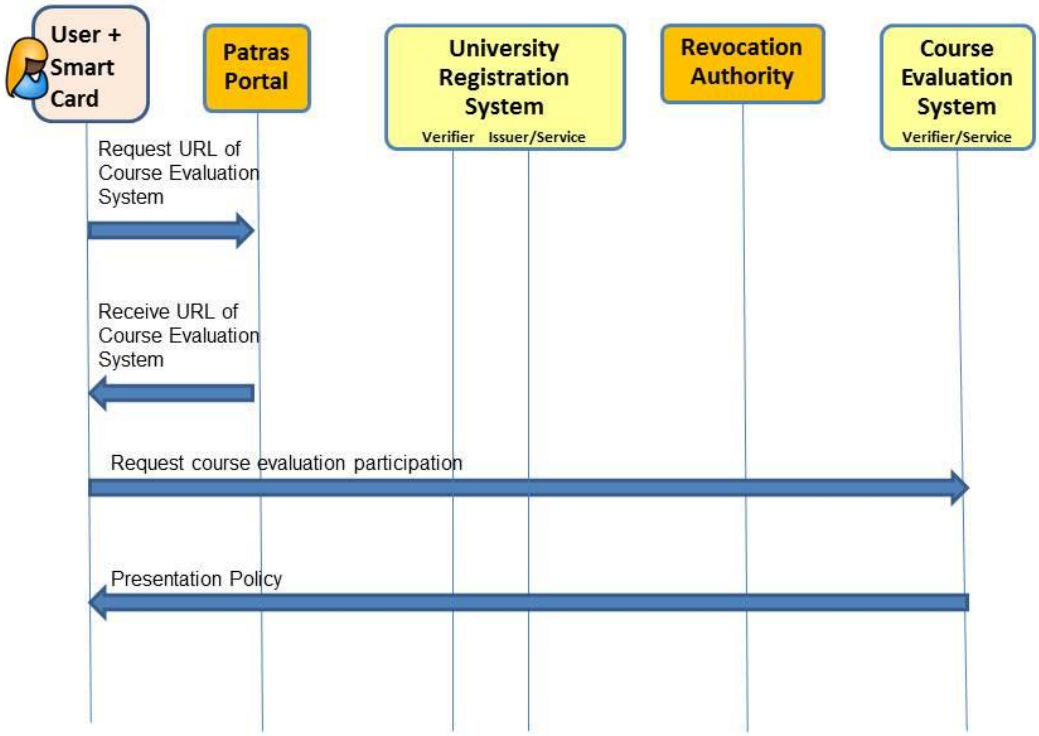

Figure 18: Course Evaluation (a)

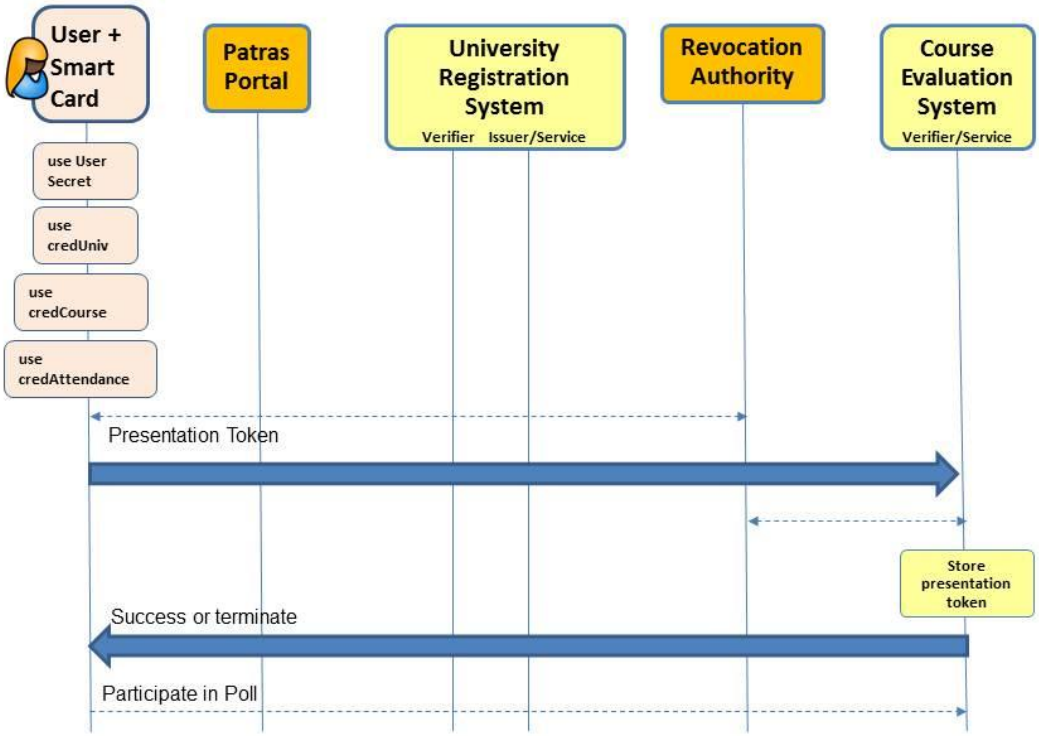

Figure 19: Course Evaluation (b)

4.6 Role Mapping

In the table below the roles are mapped according the above ABC architecture figure.

Entity	ABC Role
University Registration System	Issuer
University Student	User
User's Home Application	User Agent
Course Evaluation System.	Verifier
University Registration System	Revocation Authority
University Registration	Revocation Requestor

Office	

Table 4: ABC Role Mapping for the Course Rating by Certified Students Pilot

Below we give a detailed description of the mapped entities according ABC architecture:

Issuer: The ABC role Issuer defines that system component that issues Privacy-ABCs containing attributes to users. In the "Course Rating by Certified Students" scenario that component is the University Registration System. The users of the system i.e. students of Patras University contact this system in order to collect a Privacy-ABC that guarantees their validity as students of the specific university. Moreover, when students desire to book a course they interact with this component in order to get issued a Privacy-ABC which specifies that they have officially registered to this course.

In order to issue university and course credentials to students, the University Registration System must know the personal data of the students that will participate in the Patras pilot. This personal data will be provided by the Department's Registration Office to CTI who will act as a data controller. Additionally, the University Registration System will consist of sub-components (e.g. IdM) that will be developed and administrated by NSN. However, CTI will act as a data processor since the system will be integrated and operated in its premises by authorized CTI employees.

Finally, the Class Attendance System consists of a second Issuer in the Patras pilot as it issues attendance credentials to the students that attend a specific lecture of a course. This component does not need to know any student attributes.

User: The role User defines the human entity that collects Privacy-ABCs from an Issuer and wants to access a resource controlled by a Verifier. When interacting with an Issuer a User takes the role of Credential Receiver and when she desires to access a resource through a Verifier, she acts as a Prover.

The Users in the Patras pilot are the students that will participate in the trial. In order to interact with the pilot's Issuer and Verifier, the students are represented by a software component called User Agent. This software component runs locally on their PCs and enables them to use and browse the Privacy-ABCs stored on their smart cards.

User Agent: This is a software component that represents the human User and manages her credentials. In the "Course Rating by Certified Students" scenario, this component is depicted on the pilot architecture figure and is called User's Home Application.

Verifier: The ABC role Verifier defines the system component that protects the access to a resource or a service. By presenting a policy to Users, it imposes restrictions on the credentials they must own and the information from these credentials that they have to reveal in order to access the service. The Verifier accepts credentials from Issuers that she trusts.

In the "Course Rating by Certified Students" scenario the component that acts as a Verifier is the Course Evaluation System. This component is using an ABC System in order to grant access to the Course Evaluation Application only to those Users (i.e. students) that satisfy certain properties (e.g. have booked the course, have attended a minimum number of course lectures). The Issuers that this Verifier trusts are the University Registration System and the Class Attendance System.

Revocation Authority: A Revocation Authority is an entity that is responsible for revoking issued Privacy-ABCs upon request of the Revocation Requestor. When a Privacy-ABC is revoked, it can no longer be used for generating presentation tokens. The revocation requestor will be the department's registration office which will present to the revocation authority a formal request with a suitable justification of the revocation request.

In the "Course Rating by Certified Students" scenario the component that implements the Revocation Authority is the University Registration System. Upon request of Revocation Requestor, a university registration office employee, using the University Registration System can revoke the requested credential.

Revocation Requestor: A Revocation Requestor is an entity that requests to the Revocation Authority to revoke a certain Privacy-ABC.

In this pilot the entities that can request for the revocation of a credential are Users (i.e. student) and the university registration office employees. A university registration office employee can revoke a student Privacy-ABC under certain circumstances e.g. when the student has graduated or she has unsubscribed from the university. A student can request for her university credential to be revoked e.g. in case her smart card is lost or stolen.

Mapping of roles in the sense of the data protection law: Within the Patras pilot several different entities are involved. Some entities act in different phases or relations to other entities. Depending on the activity such entities may take several roles in the sense of the data protection law.[12] For example the professor or lecturer that triggers an evaluation of her lecture is data controller for the student data which she might have received and used for class administration (e.g. a mailing list for providing lecture notes or urgent information). But she would be a data subject in regard to the data provided during the evaluation as the information regarding the quality of the lecture directly relate to her person.

While the mapping of the ABC roles above is necessary prerequisite to understand the data flows and functionality of the system used in the pilot the mapping of the legal roles has other objectives: The legal roles bring either responsibilities or rights. As for the data controller the most important legal consequence is to bear the responsibility for the compliance with data protection rules (see [Art29WP169] page 4). It also determines the applicable national law and the jurisdiction of the competent data protection authorities (see [Art29WP169] page 5). It thereby is possible to have that several data controllers determine the purpose of the processing and thus are joint controllers for this respective data.

In the table below the roles are mapped according to the state of the development at the editorial deadline of this document. As the pilot is still under development the final distribution of tasks may be different and the mapping is subject to changes.

Entity	legal role	comment
Department Registration Office acting as student administration office	data controller	The Department Registration Office is part of the university. It processes the data on its own behalf for own purposes (administering the students and classes, distributing students to classes). It therefore determines the scope and means of the processing.
CTI[13] operating the IdM directory	data controller	CTI is the legal entity running the Patras pilot. CTI determines the means and purposes of processing and the details of the pilot.

[12] Other areas of law such as private law are not object of this contribution.

[13] CTI is a non- profit organization, and it is supervised by the Greek Ministry of Education as a financially, administratively and scientifically independent institution.

Entity	legal role	comment
CTI collecting student data for the trial from the Department Registration Office	data controller, recipient	CTI runs the ABC4Trust Patras pilot. Based on prior informed consent CTI collects personal about the student's data from the Department Registration Office CTI therefore determines the scope and means of the collection.
Department Registration Office providing student data to CTI for the pilot's database	data controller	The Department Registration Office is part of the university. It processes the data on its own behalf for own purposes (administering the students and classes, distributing students to classes). While transferring it does not act as a data processor of CTI but rather provides own student registration data to CTI. The Department Registration Office acts on own purposes, e.g. providing aid with the research project to CTI.
NSN as operator of IdM directory	data processor	NSN operates the IdM directory and provides services via online connection in case of server failures. NSN does not have own purposes to process the personal data stored on the system. It acts behalf of CTI which is the responsible data controller while NSN takes the role of a data processor.
CTI operating the Patras Portal	data controller	Insofar as the Patras Portal requires that personal data are processed CTI is data controller. If the deployment of Privacy-ABCs makes the processing of personal data completely obsolete on the, CTI would not be a data controller for this part of the pilot.
CTI operating the Course evaluation system	data controller	Insofar as the Patras Portal requires that personal data are processed CTI is data controller. If the deployment of Privacy-ABCs makes the processing of personal data completely obsolete on the, CTI would not be a data controller for this part of the pilot. While no personal data of students is processed the system heavily processes personal data of the lecturers being evaluated.
CTI creating the high end	data controller	CTI will process the evaluation results and

Entity	legal role	comment
course evaluation results		make them available to HQAA members.
User's home (students viewing personal data in IdM database)	data subject	The processing occurs as part of the data subject's own interest and for enforcing the data subject's rights.
User collecting credentials with personal data (credUniv)	data subject	The processing occurs as part of the data subject's own interest enforcing data subject's rights. The data is under control of the User. The user has a free choice to provide the data contained in the credentials for each presentation.
User's home (students requesting rectification of personal data in IdM database)	data subject	The processing occurs as part of the data subject's own interest and for enforcing the data subject's rights.
Students collecting attendance credentials (credAttendance)	no role	Students are anonymous. As there is no personal data concerned data protection law is not applicable.
CTI providing attendance Credential	open	As the issuance system cannot identify a student and thus the student remains anonymous CTI as operator of the issuance system does not have a role. The data protection law is applicable to processing of anonymous data. However, here systems deploying Privacy-ABCs raise a new legal issue: To ensure privacy for users the systems require maintenance as well as technical and organizational measures to ensure security. Without the data protection law applicable legal possibilities to enforce these requirements appear to be limited to private law relations between Users and the respective service provider – which are again hard to enforce for anonymous Users.
Lecturer teaching a class that will be evaluated having a list of students, enrolment for exams, list of grades etc.	data controller	purpose: teaching, class administration (the list is not mandatory for the lecturer to have it in class but it helps the lecturer estimate attendance volume and proceed, accordingly, to a number of administration duties e.g. photocopying lecture notes, distributing course books etc.)
Lecturer as person which is	data subject	The lecturer and her performance are

Entity	legal role	comment
object of the evaluation		evaluated by the students. While the system does not collect personal data from students it is designed to collect such data about the lecture and about the person of the lecturer herself.
Lecturer grading an exam paper	data controller	Legal entity is either the chair or the university. A transfer of grades to the rating system or portal requires a legal ground.
CTI allowing HQAA access to the evaluation results	data controller	
HQAA	data controller	Accesses evaluation results which are personal data of the lecturer as part of the legally assigned task of this authority to evaluate and assess the quality of higher education on Greek universities (purpose). HQAA is responsible for the personal data collected.

Table 5: Legal Role Mapping for the Course Rating by Certified Students Pilot

5 Requirements

Having the two specific pilots chosen will give us the opportunity to test Privacy-ABCs use and performance with two user groups of differing skills and needs. Furthermore the direction of information exchange differs with respect to whose anonymity is protected and the structure of information exchange differs (form-based in Greece vs. free-form chatting in Sweden). In this sense, the two trials are complementary and will provide feedback of distinct value to the developers of the reference implementation. Accordingly, the two pilots have different requirement sets as well as some shared ones, which we are going to provide in this section.

Also, it should be remarked that the requirements put forth in this deliverable are ABC specific and do not cover general pilot software requirements (e.g. web technology used, user GUIs, interfaces etc.). These requirements and corresponding adopted solutions will be discussed, separately, in deliverables D6.2 and D7.2 (of the pilot work packages WP6 and WP7 respectively) where the pilot application software and engineering decisions will be described in full detail along with ABC specific implemented functionality.

It should be stated, that the interim counter-based approach for obtaining 'attendance data' for the Patras Pilot is out-of-scope of ABC technology and will therefore not be mentioned in this deliverable.

Finally, standard network anonymity, network security (e.g. support of HTTP/HTPPS, TLS, SSL, high availability requirements, PKIs, firewall rules etc.) and other infrastructure requirements not directly related to ABCs are also out-of-scope of this deliverable and will be covered in the deliverables of the two pilots (WP6 and WP7).

5.1 Generic Requirements

By examining the scenario definitions of the Swedish and Greek pilots, we note that some requirements apply to both of them. In the following list, we provide these generic requirements, which will form the core elements of the common denominator description that will be given in deliverable D5.2 by month 19:

1. Every User must be provided with a contactless smart card reader and a contactless Smart Card. On top of that, in order to prove that ABC technology is not dependant on Smart Cards, 2 or 3 dummy Users will interact with the system without using Smart Cards.
2. Revocation of Privacy-ABCs must be enabled by ABC technology.
3. Privacy-ABCs must be able to be bound to the Smart Card and/or to the User.
4. The User must not be able to manipulate the presentation tokens or the Privacy-ABCs without damaging their integrity.
5. The Privacy-ABCs must be stored on the Smart Card.
6. Generating an issuance token or a presentation token must require a PIN in order to authenticate the User. (Exception: a PIN is not required when the User applies for a credAttendance credential in the Patras pilot.)
7. The User must be able to read all contents of her Smart Card except the User's Secret (the latter requirement is provided as a built-in feature by the Smart Card).
8. The User must be able to change the PIN of her Smart Card.
9. The User must be able to unlock the Smart Card by entering a PUK (similar to the mobile phone handling).

10. All processing of personal data requires a legal basis. Unless this is provided by law, informed consent of the participants is required.
11. A presentation token must be unlinkable to the Privacy-ABCs which have been used to generate it, if the User chooses to remain anonymous.
12. During the Issuance of Privacy-ABCs, the new credential must be able to contain attributes from Privacy-ABCs already owned by the User without the Issuer being able to know the value of these attributes (i.e. carry-over attributes).
13. During the Issuance of Privacy-ABCs, the new credential must be able to be bound to a User Secret such that this credential would be useless if transferred to other Smart Cards.
14. Both the Verifier and the Issuer must be able to require the User to insert a pseudonym in her token bound to the User's Secret such that the recipients of the token (i.e. Verifier and Issuer) can be sure that no one else other than this specific User can generate the chosen pseudonym.
15. The User must have the possibility to generate a token with a specific pseudonym previously used by her.
16. Both the Verifier and the Issuer must be able require the User to insert a pseudonym in her token which is not only bound to the User's Secret, but also bound to a scope (e.g. an URL). In this special case, the ABC technology must force the User to generate the same pseudonym (i.e. scope exclusive pseudonym) if the scope is the same.
17. The ABC technology must prevent Users from generating tokens from attributes not certified by their own Privacy-ABCs.
18. The ABC technology must enable all players receiving tokens for checking if the tokens are based on attributes of Privacy-ABCs owned by the Users sending the tokens.
19. A replay of the same token must not be allowed by ABC technology.
20. Log files must be generated by the ABCE which will provide input for forensics and liability issues.
21. The log files must never reveal the values of non-public keys and secrets.
22. The User must be able to generate presentation tokens based on Privacy-ABCs which were issued by different issuers.
23. When the pilots are over, it must be possible to delete all the data stored about the Users in the system (including the smart cards).
24. Personal data must be deleted once it is not needed anymore. For this, deletion periods and a deletion process must be defined.

5.2 Söderhamn Requirements

The most important requirements of the School Pilot are described in the following list:

1. For the Söderhamn Pilot, 1050 Smart Cards with full functionality must be supplied.
2. The School Registration System must contain a minimal subset of certified attributes for the pupils.
3. After successfully logging in to the School Registration System, Users must be able to edit some of their personal attributes.
4. Every Inspector must be provided with a contactless smart card reader and a contactless Smart Card.

5. Inspection must require a PIN in order to authenticate the Inspector.
6. A User must have one main credential (i.e. credSchool) and multiple 'auxiliary' Privacy-ABCs (i.e. credRole, credGuardian, credChild, credClass and credSubject).
7. The school credential (credSchool) must be bound to the User Secret.
8. Every credential of type credRole must contain only one role value. Every user will have at least one credRole credential.
9. Every credential of type credGuardian must contain only one guardian value. Every pupil will have at least one credGuardian credential, each one attesting the civic registration number of one guardian.
10. Every credential of type credChild must contain only one child value. Every guardian will have at least one credChild credential, each one attesting the civic registration number of one child.
11. Every credential of type credClass must contain the attribute values of only one class of a specific year. Every pupil will have at least one credClass credential attesting which grade and which class the pupil belongs to in a specific year.
12. Every credential of type credSubject must contain only one subject value. Every pupil will have at least one credSubject, each one attesting one subject she is learning.
13. Informed consent is required by pupils and parents before the processing of personal data begins.
14. Age of the pupils and capability of comprehension must be considered for user interfaces as well as for legal and information material.
15. Inspection of inspectable attributes must be enabled (see deliverable D2.1, Section 2.6 [DAACT]).
16. Inspectable (verifiably encrypted) attributes in the presentation tokens must not be linkable even if the attribute values prior to encryption are the same (e.g.: if the pupil generates a presentation token A when accessing restricted area X and a presentation token B when accessing restricted area Y, the inspectable attributes of A and B must not be the same).
17. The Verifier must not be able to decrypt inspectable attributes within presentation tokens.
18. The Verifier must be able to prove that the contents of the encrypted inspectable attributes match the requested data (i.e. the matriculation number or the civic registration number of the User).
19. Multiple Inspectors with different Inspectors' secret keys must be supported.
20. The same inspectable attribute must be able to be encrypted multiple times (e.g.: Inspector A is the headmaster and Inspector B is a nurse. Now if a pupil enters a restricted area to communicate with nurse B (who is both a User and an Inspector), the pupil can be requested to encrypt the inspectable attribute first using Inspector B's (the nurse's) public key and then encrypt the result using Inspector A's public key. In case of an emergency situation, the nurse will forward the pupil's presentation token to Inspector A, who checks the inspection grounds. If Inspector A decides to apply her secret key, she forwards the result to the nurse who then can uncover the identity of the pupil by applying her own secret key).
21. Inspection Grounds must be bound to the inspectable attribute.
22. Inspection Grounds must be clearly defined beforehand. Generally inspection grounds should be part of the information provided before the pilot starts. If during the pilot period changes become necessary this is possible as each creation of a presentation token that allows inspection requires an individual consent.

23. The inspection process must be protected from excessive access by appropriate means such as
    - requiring the sequential or concurrent interaction of several inspectors for performing the inspection

      or

    - 'break-the-glass' mechanisms that ensure the detection that an inspection has been performed.
24. The User must be able to offer a single presentation token containing n inspectable attributes of the same attribute value (e.g. the civic registration number) which n different Inspectors could independently decrypt if the corresponding (and perhaps different) inspection grounds applies.
25. The inspection grounds must not be modifiable by the User, the Verifier or the Issuer once a presentation token has been created based on them.
26. If the Verifier requests the User to prove one of a list of predicates, the User must be able to choose which of these predicates she will prove (i.e. 'equals one of' or 'set membership') instead of providing the proofs of all.
27. Access to a Restricted Area must be per default anonymous.
28. If a Verifier requires a pupil to identify herself prior to granting her access to a Restricted Area, the pupil must be requested to explicitly agree upon this.
29. ABC technology must support the generation and verification of the proof described in section 3.4.7

5.3 Patras Requirements

In the following we describe the requirements of the University Pilot as imposed by the definition of the scenarios.

1. For the On-Site-Testing, 5-10 Smart Cards with reduced functionality will be supplied for the pilot.
2. For the first round, 25 Smart Cards with full functionality will be supplied.
3. For the second round, 25 Smart Cards with full functionality will be supplied.
4. Issuing credAttendance credentials requires battery backed-up laptops or servers with ABC technology. If fixed-installed servers are used, they must be physically secured (e.g. caged).
5. The User must have the possibility of performing a backup and a restore of the attendance data in both rounds. Restoring attendance data must be possible after receiving a new Smart Card with a new User Secret, but it must be guaranteed that the attendance data can only be used (for taking part in the course evaluation) by Users who originally received it.
6. ABC technology must support the generation and verification of the proof described in section 3.4.7
7. The University Registration System must contain a minimal subset of certified attributes for the students.
8. After successfully logging in to the University Registration System, students must be able to edit some of their personal attributes.
9. When a university credential is being issued, a revocation handle must be inserted for revocation purposes.

10. The university credential (credUniv) must be bound to the User Secret.
11. The class attendance system must be installed on a laptop or a server with sufficient battery power. This offline-system must be pre-configured by CTI prior to every lecture and removed from the lecturing room after the lecture.
12. Multiple Class Attendance Systems must be available for the students when leaving the lecturing room. Therefore a single student must be able to process credAttendance credentials from different issuers.
13. In order to collect attendance data, the students must not be requested to enter their PINs.
14. The students must get a positive indication if she successfully received the attendance data.
15. The students must get a negative indication if there was an error in receiving the attendance data.
16. The User must be able to make a backup of her credAttendance Privacy-ABCs on trusted hardware
17. The User must be able to restore the credAttendance Privacy-ABCs on her new Smart Card
18. A student must only be able take part in the course evaluation process if she possesses the following Privacy-ABCs:
    a. credUniv
    b. credCourse
    c. sufficient number of different credAttendance credentials
19. ABC technology must support the generation and verification of the proof described in section 4.4.4.
20. The User must be able to generate a presentation token with a new Smart Card based on restored credAttendance credentials which were issued to her before she lost her old Smart Card.
21. User must be able to generate a presentation token based on credAttendance credentials, a credUniv credential and a credCourse credentials which were issued by different issuers.
22. The User can evaluate as many times as she desires during the evaluation period. ABC technology must enable the course evaluation system to take only her last evaluation into account even though she posted her evaluation without revealing her identity.

6 Glossary

Anonymous

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

Attribute

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

Certified pseudonym

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

Credential

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

Credential specification

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

Data Controller

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

Data Processor

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

Data Subject

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

Device binding

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

Entity

Entity is anything that has a distinct existence; it is the fundamental "thing" that can be identified.

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

Inspection

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

Inspection grounds

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

Inspection Requester

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

Inspector

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

Issuance key

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

Issuer

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

Issuer parameters

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

Linkability

See *unlinkability*.

Personal data

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

Personally Identifiable Information (PII)

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

used terminology for *personal data* in the domain of information security. Within this document PII is used in relation to information security.

Presentation policy

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

Presentation token

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

Pseudonym

See *verifiable pseudonym*.

Pseudonym scope

A string provided in the Verifier's presentation policy as a hint to the User which previously established pseudonym she can use, or to which a new pseudonym should be associated. A single User (with a single user secret) can generate multiple verifiable or certified pseudonyms for the same scope string, but can only generate a single scope-exclusive pseudonym.

Pseudonymous

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

Revocation

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

Revocation Authority

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

Revocation information

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

Revocation parameters

The public information related to a Revocation Authority, containing cryptographic information as well as instructions where and how the most recent revocation information and non-revocation evidence can be obtained. The revocation parameters are static, i.e., they do

not change every time a new credential is revoked or at regular time intervals like the revocation information and non-revocation evidence (may) do.

Non-revocation evidence

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

Scope

See *pseudonym scope.*

Scope-exclusive pseudonym

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

Traceability

See *untraceability*.

Unlinkability

The property that different actions performed by the same User, in particular different presentation tokens generated by the same User, cannot be linked to each other as having originated from the same User.

Untraceability

The property that an action performed by a User cannot be traced back to her identity. In particular, the property that a presentation token generated by a User cannot be traced back to the issuance of the credential from which the token was derived.

User

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

User agent

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

User binding

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

User secret

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

Verifiable pseudonym

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

Verifier

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

7 Acronyms

ABCs
: Attribute Based Credentials

Privacy-ABCs
: Privacy Attribute Based Credentials (privacy ABCs)

ABCE
: ABC Engine

CA
: Certificate Authority

CE
: Crypto Engine

DFD
: Data Flow Diagrams

GUI
: Graphical User Interface

HTTP
: Hypertext Transfer Protocol

HTTPS
: HyperText Transfer Protocol Secure (HTTP secured by TLS or SSL)

HQAA
: Hellenic Quality Assurance Agency

ID
: Identifier

Idemix
: IBM Identity Mixer

IdM
: Identity Manager

ISP
: Internet Service Provider

NFC
: Near Field Communication

PC
: Personal Computer

PIN

Personal Identification Number

PUK

PIN Unlock Key

RP

Relying Party

SC

Smart Card

SCI

Smart Card Interface

SSL

Secure Sockets Layer

STS

Secure Token Service

TTP

Trusted Third Party

TLS

Transport Layer Security

URI

Uniform Resource Identifier

WP

Work Package

XML

eXtensible Markup Language

8 Bibliography

[Art.29WP136] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, Adopted on 20th June 2007, 2007, online:

http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm

[Art.29WP148] Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines*, Adopted on 4 April 2008", 2008, online:

http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm

[Art29WP163] Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, Adopted on 12 June 2009, 2009, online:

http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009_en.htm

[Art29WP169] Article 29 Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor',* Adopted on 16 February 2010, online:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[Car09] Peter Carey, *Data Protection – A Practical Guide to UK and EU Law*, 3rd ed., Oxford, 2009.

[FAC04] https://www.facebook.com/

[GolSch10] Peter Gola, Christoph Klug, Barbara Körrffer, Rudolf Schomerus, *BDSG Bundesdatenschutzgesetz*, 10th ed., Munich, 2010.

[JaRo11] Silke Jandt, Alexander Roßnagel. Datenschutz in Social Networks – Kollektive Verantwortlichkeit für die Datenverarbeitung, in Zeitschrift für Datenschutz (ZD), p. 160-166, 2011.

[JCBHWZ09] David-Olivier Jaquet-Chiffelle, Emmanuel Benoist, Rolf Haenni, Florent Wenger und Harald Zwingelberg, "Virtual Persons and Identities", in Kai Rannenberg, Denis Royer, André Deuker (Eds.) *The Future of Identity in the Information Society*, Springer, 2009, online:

http://www.springerlink.com/content/j111742738714u37

[KarTho11] Moritz Karg, Sven Thomsen. *Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook*, Kiel, Germany, 2011, online:

https://www.datenschutzzentrum.de/facebook/

[DAACT] Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin and Harald Zwingelberg. D2.1 Architecture for Attribute-based Credential Technologies, 2011 https://abc4trust.eu/index.php/pub/107-d21architecturev1

[KrüMau11] Stefan Krüger, Svenja-Ariane Maucher. Ist die IP-Adresse wirklich ein personenbezogenes Datum? - Ein falscher Trend mit großen Auswirkungen auf die Praxis, in *Multimedia und Recht* (MRR) 2011 pp. 433-439, online: http://beck-online.beck.de/Default.aspx?vpath=bibdata%2fzeits%2fMMR%2f2011%2fcont%2fMMR.2011.433.1.htm

[KuLeBe10] Aleksandra Kuczerawy, Ronald Leenes, Bibi van den Berg. Legal aspects of social network sites and collaborative workspaces, in Bibi van den Berg, Ronald Leenes (Eds.), PrimeLife Deliverable D1.2.1 *Privacy Enabled Communities*, 2010, online:

http://www.primelife.eu/results/documents/95-121d

[PfiHan10] Andreas Pfitzmann, Marit Hansen. *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, Dresden and Kiel, Germany, 2010, online: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[Sim11] Sipros Simitis [ed.]. *Bundesdatenschutz*, 7th ed., Nomos, Baden Baden, Germany, 2011.

[Zwi11] Harald Zwingelberg. Necessary processing of personal data: The need-to-know principle and processing data from the new German identity card. In Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, and Ge Zhang, editors, *Privacy and Identity Management for Life*, volume 352 of *IFIP Advances in Information and Communication Technology*, pages 151–163. Springer Boston, 2011.