# *D6.1 Application Description for the School Deployment*

Souheil Bcheri, Norbert Goetze, Monika Orski,
Harald Zwingelberg

| | |
|---|---|
| *Editors:* | *Monika Orski (Eurodocs)* |
| *Reviewers:* | *Joerg Abendroth (Nokia-Siemens Networks), Gregory Neven (IBM)* |
| *Identifier:* | *D6.1* |
| *Type:* | *Deliverable* |
| *Version:* | *1.1* |
| *Date:* | *06/03/2012* |
| *Status:* | *Final* |
| *Class:* | *Public* |

Abstract

The Söderhamn school pilot will use ABC technologies to anonymously verify credentials and give pupils access to chats, online counselling sessions and document areas based on these credentials, e.g. age, gender or form.

This document describes the requirements for the Söderhamn school pilot, the project plan for implementing it, and the overall architecture of the pilot.

*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 |

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

# List of Contributors

| **Chapter** | **Author(s)** |
|---|---|
| Executive Summary | Monika Orski (EDOC) |
| Introduction | Souheil Bcheri (EDOC), Monika Orski (EDOC) |
| Chapter 2 | Souheil Bcheri (EDOC), Monika Orski (EDOC), Harald Zwingelberg (ULD) |
| Chapter 3 | Souheil Bcheri (EDOC), Norbert Goetze (NSN), Monika Orski (EDOC) |
| Chapter 4 | Souheil Bcheri (EDOC), Monika Orski (EDOC) |
| Chapter 5 | Souheil Bcheri (EDOC), Monika Orski (EDOC) Eva Schlehahn (ULD), Harald Zwingelberg (ULD) |
| Chapter 6 | Norbert Goetze (NSN), Monika Orski (EDOC) |
| Chapter 7 | Monika Orski (EDOC) |

# Foreword 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 system deploying Privacy-ABCs that will be integrated into two complete real pilot applications providing feedback to the reference architecture and implementation results. These will be the first pilots of Privacy-ABC deployments in real application environments for collecting feedback.

This document relates to one of the ABC4Trust pilots, the school pilot in Söderhamn, Sweden. The pilot implements ABC in the protection of the anonymity of children in a school environment located in Söderhamn, Sweden.

In this document, we address the different areas of the pilot's functions, and also the overall architecture, including both IdM components and the part specifically made for this pilot. Functional requirements are listed at a general level, and detailed in use cases. Also, the general GUI layout is shown, mostly in screen dumps from the system already under construction, and the functional and non-functional requirements for the Söderhamn pilot are described.

# Table of Contents

1 Introduction ........ 10

1.1 The ABC4Trust Project ........ 10
1.2 Objectives and Rationale for the Pilot ........ 11
1.3 Main Pilot Functions ........ 11
1.4 Pilot Objectives ........ 12
1.5 Structure of the Document ........ 13

2 General Functional Requirements ........ 14

2.1 Concepts ........ 14
2.2 User Types and Actor Roles ........ 14
2.3 Mapping of ABC Roles ........ 15
2.4 School Pilot Functions ........ 17
2.5 Scenarios ........ 17

2.5.1 Counselling ........ 17

2.5.2 Restricted Chat Room ........ 18

2.5.3 Political Discussions ........ 18

2.5.4 Sharing Documents ........ 19

2.5.5 An Emergency Situation ........ 19

2.6 Who Sees What ........ 19

3 Use Cases Summaries ........ 21

3.1 ABC System Setup ........ 21
3.2 School Pilot Registration I (Bootstrap) ........ 23
3.3 School Pilot Registration II ........ 24
3.4 Other School Credentials ........ 25
3.5 Viewing User's Data ........ 26
3.6 Instantiating a Restricted Area ........ 27
3.7 Access to a Restricted Area ........ 28
3.8 Counselling ........ 29
3.9 Restricted Chat Room ........ 30
3.10 Political Discussions ........ 32
3.11 Sharing Documents ........ 33
3.12 Polling ........ 34
3.13 Revocation ........ 35
3.14 Emergency Situation ........ 36
3.15 Viewing/Deleting Credentials ........ 37
3.16 Changing PIN ........ 38
3.17 Unlocking the SC ........ 39

4 GUI Views ........ 40

4.1 User GUI of Restricted Area ........ 40
4.2 Administration GUI of Restricted Areas ........ 47

4.2.1 Access policy builder ........ 50

5 Non-functional Requirements ........ 53

5.1 System Requirements ..... 53
5.2 Defining security and data protection requirements via protection goals ..... 53
5.3 Data protection and data security related requirements ..... 55
5.3.1 Generic data protection requirements for the pilot ..... 55
5.3.2 Use case specific data protection requirements ..... 57
5.4 Volume and Performance Expectations ..... 62
5.5 Other Non-functional Requirements ..... 62
5.6 Credentials ..... 63
6 Architecture of the School Pilot ..... 66
6.1 System Overview ..... 66
6.2 Restricted Area System Architecture ..... 67
6.3 IdM Portal Architecture ..... 68
6.4 IdM Application Architecture ..... 69
7 Project Plan ..... 70
7.1 Time Line ..... 70
7.2 Software Development Roles needed ..... 70
7.3 Iterations ..... 72
7.3.1 Iteration 1 ..... 72
7.3.2 Iteration 2 ..... 72
7.3.3 Iteration 3 ..... 73
7.3.4 Pre-pilot ..... 73
8 Glossary ..... 74
9 Acronyms ..... 79
10 Bibliography ..... 81

1 Introduction ..... 10
1.1 The ABC4Trust Project ..... 10
1.2 Objectives and Rationale for the Pilot ..... 11
1.3 Main Pilot Functions ..... 11
1.4 Pilot Objectives ..... 12
1.5 Structure of the Document ..... 13
2 General Functional Requirements ..... 14
2.1 Concepts ..... 14
2.2 User Types and Actor Roles ..... 14
2.3 Mapping of ABC Roles ..... 15
2.4 School Pilot Functions ..... 17
2.5 Scenarios ..... 17
2.5.1 Counselling ..... 17
2.5.2 Restricted Chat Room ..... 18
2.5.3 Political Discussions ..... 18
2.5.4 Sharing Documents ..... 19

2.5.5 An Emergency Situation ........ 19

2.6 Who Sees What ........ 19

3 Use Cases Summaries ........ 21

3.1 ABC System Setup ........ 21
3.2 School Pilot Registration I (Bootstrap) ........ 23
3.3 School Pilot Registration II ........ 24
3.4 Other School Credentials ........ 25
3.5 Viewing User's Data ........ 26
3.6 Instantiating a Restricted Area ........ 27
3.7 Access to a Restricted Area ........ 28
3.8 Counselling ........ 29
3.9 Restricted Chat Room ........ 30
3.10 Political Discussions ........ 32
3.11 Sharing Documents ........ 33
3.12 Polling ........ 34
3.13 Revocation ........ 35
3.14 Emergency Situation ........ 36
3.15 Viewing/Deleting Credentials ........ 37
3.16 Changing PIN ........ 38
3.17 Unlocking the SC ........ 39

4 GUI Views ........ 40

4.1 User GUI of Restricted Area ........ 40
4.2 Administration GUI of Restricted Areas ........ 47

4.2.1 Access policy builder ........ 50

5 Non-functional Requirements ........ 53

5.1 System Requirements ........ 53
5.2 Defining security and data protection requirements via protection goals ........ 53
5.3 Data protection and data security related requirements ........ 55

5.3.1 Generic data protection requirements for the pilot ........ 55

5.3.2 Use case specific data protection requirements ........ 57

5.4 Volume and Performance Expectations ........ 62
5.5 Other Non-functional Requirements ........ 62
5.6 Credentials ........ 63

6 Architecture of the School Pilot ........ 66

6.1 System Overview ........ 66
6.2 Restricted Area System Architecture ........ 67
6.3 IdM Portal Architecture ........ 68
6.4 IdM Application Architecture ........ 69

7 Project Plan ........ 70

7.1 Time Line ........ 70
7.2 Software Development Roles needed ........ 70
7.3 Iterations ........ 72

7.3.1 Iteration 1 ........ 72

7.3.2 Iteration 2 ........ 72

7.3.3 Iteration 3 .......... 73
7.3.4 Pre-pilot .......... 73
8 Glossary .......... 74
9 Acronyms .......... 79
10 Bibliography .......... 81

# Index of Figures

Figure 1: School web application – List of available chat rooms ....40
Figure 2: School web application – Access policy to meet....41
Figure 3: School web application – Wall ....42
Figure 4: School web application - Documents ....43
Figure 5: School web application - Chat....44
Figure 6: School web application – On-screen privacy mode is switched ”Off”....45
Figure 7: School web application – On-screen privacy mode is switched ”On” ....46
Figure 8: School web application - Administration section - List of Restricted Areas....47
Figure 9: School web application - Administration section – Configuration of a Restricted Area details (part 1 of 2)....48
Figure 10: School web application - Administration section – Configuration of a Restricted Area details (part 2 of 2) ....49
Figure 11: School web application - Administration section - Access Policy list ....50
Figure 12: School web application - Administration section - Access Policy Builder (building policy “boys 10 years”) ....51
Figure 13: School web application - Administration section – Configuration of predefined access policies....52
Figure 14: High Level Architecture/Söderhamn Pilot....66
Figure 15: IDM Portal and IDM Application Architecture....68
Figure 16: Overall timeline ....71
Figure 17: Development iterations and pre-pilot timeline ....71

# 1 Introduction

Over the past 10-15 years, a number of technologies have been developed to build ABC systems in a way that they can be trusted, like normal cryptographic certificates, while at the same time protecting the privacy of their holder (e.g., hiding the real holder's identity). Such Attribute-based credentials (ABCs) are issued just like ordinary cryptographic credentials using a digital (secret) signature key.

The ABC4Trust project aims to run pilots of ABC deployments in production environments. Thus it will provide an opportunity to provide real user feedback on Privacy-ABC systems. ABC4Trust will gather practical experience with ABC applications in two specific environments. Having these two specific pilots will give the opportunity to test credentials use and performance with two user groups of differing skills and needs. One of the groups will be users at a school in Söderhamn, Sweden. This pilot will provide feedback of distinct value to the developers of the reference implementation.

The Swedish pilot in Söderhamn will consider several types of communication needed by the school: chat rooms to be used by pupils and/or staff, online counselling sessions where staff can provide counselling in a safe environment while pupils are not required to state their identity, and document areas where staff can share documents (e.g. grades and development plans) with pupils and their guardians.

## 1.1 The ABC4Trust Project

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

1. Produces an architectural framework for ABC technologies that allows different realizations of these technologies to coexist, be interchanged, and federated
   a. Identify and describe the different functional components of ABC technologies, e.g. for request and issue of credentials and for claims proof;
   b. Produce a specification of data formats, interfaces, and protocols formats for this framework;
2. Defines criteria to compare the properties of realizations of these components in different technologies; and
3. Provides reference implementations of each of these components.

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

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

## 1.2 Objectives and Rationale for the Pilot

As a European project, ABC4Trust aims to address the federation and "interchangeability" of technologies that support trustworthy, yet privacy-preserving, Attribute-Based Credentials. On the other hand, it will help deepening the understanding in ABC technologies, enabling their efficient and effective deployment in practice, and their federation in different domains.

By taking into account the collection of criteria and the design and implementation of the necessary infrastructure (Identity Service Provider, infrastructure to issue credentials [e.g. with smart cards], attribute databases, etc.), the evaluation of the pilot will provide a clear proof of concept of both the unified anonymous credentials idea (harmonization of various ABC protocols) as well as the reference architecture, providing at the same time feedback for enhancements.

Today, Swedish schools mainly use the public Internet as the means of communication. This leaves them a lack of protecting the privacy of pupils and their guardians, e.g. if the same username is used in sensitive and everyday use matters it is dangerous.

Swedish schools are also, according to laws and regulations, obliged to inform the guardians when a pupil is absent from a class. In addition, schools are obliged to create individual plans for each student. Individual plans contain private data and very sensitive information about a child's ability to read, ability to write and other important skills, wishes and goals for the future.

The school pilot will use Privacy-ABC to enable secure identification in communications between staff, pupils and guardians. The ABC4Trust technology takes into account the three aspects identity, anonymity and privacy and combines them into one single solution.

The first pilot application at a Swedish school will involve pseudonymous community access and social networking for school students (pupils). This pilot addresses the specific challenges posed by the fact that Internet users get ever younger and often are minors. Swedish schools today are mainly using the Internet for communication between teachers, pupils and parents. They are using different portals, operated by private companies with conflicting business, and private communities to make this communication possible. A big threat to the privacy of the pupils is unauthorized access to personal information such as individual plans, presence reports, grades, exam results and other information and functions available through the school portal. Several applications, such as social networking or anonymous student counselling or medical advice will benefit from the ABC4Trust-project as it allows combining strong authentication and privacy protection into one solution. The proposed community will protect the pupil's 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 the school personnel that it communicates with authorized pupils of the respective school, gender, age or form. The pilot will help to gather information on the usability of the proposed ABC system under especially challenging usability conditions posed by children users, hardly willing to read manuals or use a many-step procedure to enter a school site.

## 1.3 Main Pilot Functions

The main scenarios for the Swedish pilot are

- Communicating and socializing via
    1. Chat
    2. Forum
- Political discussions

- Counselling with health personnel (counsellors, 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 therefore have the choice 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.

## 1.4 Pilot Objectives

The objectives for the Söderhamn school pilot are:

- Define success criteria and detailed plans for the school community application
- Collect feedback from users about the usability and the perceived privacy properties of the system
- Provide feedback to the architecture and reference implementation WPs
- Provide evaluation results to Users, Identity Service providers, and Application Providers.

The 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.

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 a forum available at the school portal.

The Swedish Pilot will develop a new Web Based School Community Application to be used for chat communication, counselling, 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 (explained in the Concepts part of the General Functional Requirements chapter).

The major challenges are that the School Community Application needs to offer many different functionalities needed by the many different scenarios such as chat, counselling, 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.

As the underlying system is also been used in a different scenario, it is generic enough for wider deployment.

## 1.5 Structure of the Document

The rest of the document is organized as follows:

Chapters 2 - 5 contain the school pilot's functional and non-functional requirements, using several views to pinpoint the requirements.

Chapter 6 outlines the technical architecture of the school pilot.

Chapter 7 describes the project plan for the development project, intended to implement the school pilot.

Chapters 8 and 9 contain a glossary and a list of acronyms.

# 2 General Functional Requirements

The main functions of the school pilot will be to let users create and use general chats, counselling sessions, and document areas. In order to do this, the concepts and user types described below will be implemented.

## 2.1 Concepts

A ***Restricted Area (RA)*** is the internal representation of every kind of chat or documents area. When an RA is created, it is defined to contain a general chat, a political discussions chat, a counselling session or a document area.

A general ***Chat*** is simply a chat area. It can be created by any user. Those using the chat remain anonymous, unless they choose to disclose their identity by showing the name stored in their credentials.

A ***Counselling Session*** is a chat where one or more members of staff provide counselling via the chat. The staff providing counselling is always identified, while the pupils using the chat remain anonymous. Only staff members can create a counselling session.

A ***Political Discussion*** chat is like a general chat, except that users remain anonymous at all times.

A ***Document Area*** is an RA where documents can be shared between staff, pupils and guardians. Only staff members can create a Document Area.

***Restrictions*** specify the access policy of a specific RA. For example, there may be a general chat only for girls in class 8A, or a specific document area for each pupil, accessed by the pupil, staff and the pupil's guardians.

***Alias*:** Within Restricted Areas, in particular in Chats and Discussion boards, Users are represented by a self-chosen nickname, their alias. Each alias can be chosen only once. The alias will be bound to the User credential while preserving unlinkability allowing the User to reclaim the alias for subsequent visits.

## 2.2 User Types and Actor Roles

The following actor roles will be used in the school pilot:

***Administrator***

Administrators can create new users, add and remove user credentials, and create and revoke user smart cards.

***User***

A User is simply someone who is allowed to log into the system. The user has a smart card to enable login. Each user belongs to one of three user groups, or types: Staff, pupil or guardian.

Members of staff then have one or more subtype, e.g. teacher or nurse.

Each pupil has a connection to one or more guardians.

Each guardian has a connection to one or more pupils.

***Inspector***

The Inspector can view the identity of each user, thus being able to trace the origin of anything posted in a chat. The inspector also uses a smart card, albeit different from that of ordinary users.

The inspector is called to take action only if some serious transgression has been reported.

***System Administrator***

The System Administrator is the person who performs the initial system start-up. This is also the role able to add new schools to the system in a future scenario containing more than the first pilot.

## 2.3 Mapping of ABC Roles

The roles that exist within a system deploying Privacy-ABCs have been described in Deliverable D5.1. These roles describe an entity performing an action with or relevant for the level of Privacy-ABCs. The entities participating in the trail have been identified to have the following roles:

| **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 authorities | Inspection Receiver |

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

**Issuer:** The ABC role Issuer defines the system component which issues Privacy-ABCs containing attributes of 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.

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

**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 circumstances 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.

We expect that 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 no longer functional. 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 the IdM application and IdM Portal to grant access to those Users that satisfy the access policy for a given restricted area. The Issuer that this Verifier trusts is the school administration office – which is the only issuer within the pilot.

**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. To authenticate towards the Verifier the User presents a presentation token to the Verifier.

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

**Inspection Requestor:** Entity requesting an inspection from the Inspector, asserting that inspection is compliant with the inspection grounds as specified or 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 for dispute resolution.

**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. To ensure that Inspection is not used maliciously within the setting of the Swedish one potential solution is to demand that that at least two persons or more act jointly (e.g. principal and data protection office). The persons that may act together to reveal the identity are called The School Inspection Board.

**Inspection Receiver:** The entity receiving the reply of the Inspection. This may be another entity than the one requesting (triggering) the inspection. E.g. in case of pupils requesting an inspection due to mobbing in the online environment it might not be necessary to let the requestor know the identity of the acting person if other means of resolving such a situation are in place.

## 2.4 School Pilot Functions

The basic functions of the school pilot will be:

- Creation of Restricted Areas of different kinds. A RA can be a chat, a counselling session, a political discussion or a document area. The RA has a set of restrictions (access policies), specifying who is allowed to enter it.
- Matching of credentials and access policies, to determine who is allowed to access a certain RA.
- Chat function. The chat function will be used in general chats as well as in counselling sessions and political discussions.
- Document upload and download, to be used within document areas.
- Attribute disclosure. A function to let the User disclose additional attributes of her credentials or even prove her identity when she chooses to do so. Staff of the school will automatically disclose their identity within the management of counselling sessions.
- Alias management. A user can choose to use an alias, within a single RA or within the system as a whole. Aliases will be unique within the system.
- Removal of content. Users can choose to remove content they previously entered from view. However, it will be retained by the system for a time (specified per RA) to be viewed by an inspector if needed.

The functional requirements are also described in the form of use cases in Chapter 3.

## 2.5 Scenarios

The different Swedish scenarios will involve pseudonymous community access and social networking or 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) against identity 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.

### 2.5.1 Counselling

In this scenario a pupil that needs counselling will be able to contact authorized professionals regarding physical and other health related problems, but also school and learning related issues. 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.

### 2.5.2 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 which can be joined by anyone who can proof the necessary attributes (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 room functionality activated. The user will also see the access policy (e.g. age between 14-15 years) for each restricted chat room. The user selects a restricted chat room and the restricted area system (in this pilot acting as the Verifier) will validate if the User' presentation token meets the criteria of the 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 further attributes.

### 2.5.3 Political Discussions

Political discussions are very important in a modern and democratic society. Young citizens should be encouraged and enabled to participate in political discourse as part of their school education. Anonymous political discussions can encourage some pupils to freely express their opinion in. This can, e.g., be useful to allow expressing dissenting opinions on sensitive subjects against a settled majority of the participants.

Political discussions are performed using restricted areas with the chat and forum functionality activated. 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 entering a discussion meets the access policy of the restricted area. The User will be anonymous. She will not be able to exchange any attributes in a verified manner even if she wishes to do so. Of course any user could still claim to be a certain person but is excluded from verifying this claim with the system, thus leaving room for denying authorship.

The inspection functionality (the possibility of revealing the identity of the user that misbehaves) is disabled in the political discussions scenario.

### 2.5.4 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 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 where these files can be picked up by the User.

Personal Restricted Areas have as a default setting only one person included in its access policy. But it is under consideration to 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.

### 2.5.5 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 are made public in advance. Before the pilot start the reasons and the definition of emergency will be finalized. The definition of an emergency situation will be part of the inspection grounds that will be published for each RA to which they are applicable.

The following steps are to be made if the inspector 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.

## 2.6 Who Sees What

The central task of the pilot is to use Privacy-ABCs to ensure authorisation as well as to protect the private sphere of the users. For this, it is important to know what part of the system processes which type of data.

The IdM Portal as part of the School Registration provides a means of obtaining the user's credentials. Users identify towards the system initially with a one-time password (OTP) and later with their user's smart card. It will not store any record of the user's communications. Cookies used will be deleted after the session. There will be no way to link users to specific communications within the IdM.

The Restricted Area System stores and transmits the content of communications, including chat and counselling. It will not, however, store any user data other than the handle that can be used to retrieve presentation tokens. There will be no way to link communications to users within the Restricted Area System. Users may use freely chosen alias names (screen names). These are stored together with the content. As users should be able re-claim "their" alias at a later visit, some information about the connection of an alias with a particular smart card will be stored in the system as well. For this purpose information will be chosen that does not allow linking the content to a particular user or other content the user might have published under another alias name.

# 3 Use Cases Summaries

This is a summary version of the use cases. Details are available internally and documented.

Each use case is identified by a unique integer sequence number identifier. The summary version uses the same number as the extensive version.

## 3.1 ABC System Setup

| | |
|---|---|
| Use Case ID: | SE_1 |
| Use Case Name: | **System Setup** |

| | |
|---|---|
| Actors: | Users<br>Inspector<br>System Administrator |
| Description: | For the actors with smartcards:<br>• These actors first need to go through this use case to initialize their smart cards and configure them to be able to participate in the other scenarios and interact with the system.<br>For the subsystems:<br>• Each subsystem that is involved with the crypto operations (e.g. issuers, revocation authorities, etc.) must be initialized with the proper parameters and secret keys. To ease this process, there will be ready scripts that the administrator needs to run on the corresponding machines. |
| Preconditions: | • All users have obtained their smart cards and their contactless smart card readers.<br>• The inspector has obtained her smart card and her contactless smart card reader.<br>• The users and the inspector have installed 'User Agent App' on their PC. |
| Postconditions: | • The system/smartcard has been initialized and can be used. |
| Normal Flow: | System Administrator:<br>1. The system administrator starts a specific script on each subsystem (e.g. issuer, revocation authority) to generate the necessary parameters and cryptographic values. .<br>User: |

| | |
|---|---|
| | 2. User places her card on her smart card reader.<br>3. The user starts the ‘User Agent App’<br>4. The user selects ‘Initialize SC’<br>5. The user is requested to authenticate to the card.<br>6. The ‘User Agent App’ performs the initialization.<br>7. The SC generates a User Secret and configures the user’s device parameters.<br>8. The SC stores the certificates and cryptographic parameters required for communicating with other parties in the system.<br>Inspector:<br>1. The inspector places her card on her smart card reader.<br>2. The inspector starts the ‘User Agent App’.<br>3. The inspector selects ‘Initialize SC’.<br>4. The inspector is requested to authenticate to the card.<br>5. The ‘User Agent App’ performs the initialization.<br>6. The SC generates the Inspector keys and configures the Inspector’s device parameters.<br>7. The inspector’s public parameters are forwarded to a storage area publicly available for all users. |

## 3.2 School Pilot Registration I (Bootstrap)

| | |
|---|---|
| Use Case ID: | SE_2_1 |
| Use Case Name: | **Obtaining the School Pilot Registration Credential** |

| | |
|---|---|
| Actors: | Users (pupils, parents, school personnel) |
| Description: | This use case describes the steps needed for a user to receive the main certificate (credential) that includes the identity information and can be used to prove that she is a registered user in the school pilot. |
| Trigger: | The user has received a new smartcard. |
| Preconditions: | • The user has obtained her smart card, her ID and her OTP.<br>• The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it. |
| Postconditions: | • The user has a credential that includes her identity information and shows that she is a registered user in the school pilot.<br>• From now on, the user is able to access her profile using her smartcard as authentication device. |
| Normal Flow: | 1. The user places her card on her contactless smart card reader.<br>2. The User selects the menu 'Get School Credential'.<br>3. The user logs in via ID and one-time-password.<br>4. The 'User Agent App' pops up.<br>5. The 'User Agent App' requests the user to authenticate to the smartcard.<br>6. The 'User Agent App' and the System run a protocol that produces a credential that includes the identity information of the user (see 5.6 for more details about the credential) and it will be stored on the smartcard. |

## 3.3 School Pilot Registration II

| | |
|---|---|
| Use Case ID: | SE_2_2 |
| Use Case Name: | **Renew School Pilot Registration Credential** |

| | |
|---|---|
| Actors: | Users (pupils, parents, school personnel ) |
| Description: | This use case describes the steps needed for a user to receive a new credential, which contains updated attributes. The obtained credential is the same as SE_2_1. |
| Trigger: | A school pilot registration attribute has changed (e.g. name. See the list of attributes in 5.6) |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it. |
| Postconditions: | • The user has a credential that includes her updated information and shows that she is a registered user in the school pilot. |
| Normal Flow: | 1. The user places her card on her contactless smart card reader.<br>2. The User selects the menu 'Update School Credential'.<br>3. The 'User Agent App' pops up.<br>4. The 'User Agent App' requests the user to authenticate to the smartcard.<br>5. The 'User Agent App' and the System run a protocol to prove the identity of the user in order to access her profile.<br>6. The 'User Agent App' and the System run a protocol that produces a credential that includes the updated information of the user (see 5.6 for more details about the credential) and it will be stored on the smartcard. |

## 3.4 Other School Credentials

| | |
|---|---|
| Use Case ID: | SE_2_3.0 |
| Use Case Name: | **Obtaining Auxiliary School Pilot Credential** |

| | |
|---|---|
| Actors: | Users (pupils, parents, school personnel ) |
| Description: | This use case describes the steps needed for a user to receive or update their auxiliary credentials (e.g. the credentials that show parent-child relationship). More details about different types of auxiliary credentials can be found in section 5.6. |
| Trigger: | One or more of the user's attributes has changed (e.g. a parent has enrolled another child into the school). |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it. |
| Postconditions: | • The user will have the desired credential stored on her smartcard. |
| Normal Flow: | 1. The user places her card on her contactless smart card reader.<br>2. The User selects the menu 'Get other School Credentials'<br>3. The 'User Agent App' pops up<br>4. The 'User Agent App' requests the user to authenticate to the smartcard.<br>5. The 'User Agent App' and the System run a protocol to prove the identity of the user in order to access her profile.<br>6. According to the information stored in the database, the possible options will be shown to the user.<br>7. The user selects the desired type of credential.<br>8. The 'User Agent App' and the System run a protocol that produces the requested credential and it will be stored on the smartcard. |

## 3.5 Viewing User's Data

| | |
|---|---|
| Use Case ID: | SE_3 |
| Use Case Name: | **Viewing of the User's Data (profile)** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel) |
| Description: | This use case describes the steps needed for viewing the user's profile.<br>The users login to the School Registration System using her smartcard and can view their data online |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it. |
| Postconditions: | |
| Normal Flow: | 1. The user selects the School Registration System<br>2. The user selects 'View Data'<br>3. The 'User Agent App' requests the user to authenticate to the smartcard.<br>4. The 'User Agent App' and the System run a protocol to prove the identity of the user in order to access her profile.<br>5. The user can view the information of her that is stored in the system. |

## 3.6 Instantiating a Restricted Area

| | |
|---|---|
| Use Case ID: | SE_5 |
| Use Case Name: | **Instantiating (=creating) a Restricted Area** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel) |
| Description: | Any user can instantiate a Restricted Area. See section 6.2 for more information about Restricted Area. |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• The user has proved he is a valid user of the system. |
| Postconditions: | • There will be a new RA in the system and the users who fulfil the access policy configured by the initiator can access this restricted area. |
| Normal Flow: | 1. The user chooses 'Setup a Restricted Area'.<br>2. The user chooses the kind of RA to be created.<br>3. If the user wants to initiate a special kind of RA that requires proof of additional user attributes (e.g. member of staff, etc.), then the user uses her smartcard to prove this fact. (For example, a counselling session can be created only if the user is a member of staff, at the request of a pupil or as session open to several pupils.)<br>4. The user will be asked for defining the access policy that must be applied when other users want to enter this restricted area.<br>5. The restricted area is created. |

## 3.7 Access to a Restricted Area

| | |
|---|---|
| Use Case ID: | SE_6 |
| Use Case Name: | **Access to a Restricted Area** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel) |
| Description: | A user can access a restricted area anonymously (default) or not anonymously (upon user's consent.<br>To access a restricted area (RA), the user must posses a number of credentials that fulfil the access policy of the RA. |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• The user has proved he is a valid user of the system. |
| Postconditions: | • The user can use the services available within this restricted area. |
| Normal Flow: | 1. The user navigates to the restricted area of her choice.<br>2. The user gets a notification about the access policy and the terms of use.<br>3. If the user accepts to the conditions, the 'User Agent App' pops up.<br>4. There 'User Agent App' askes the user to authenticate to the card.<br>5. The 'User Agent App' and the System will run a protocol to prove that the user fulfils the policy.<br>6. The user gets access to the RA. |

## 3.8 Counselling

| | |
|---|---|
| Use Case ID: | SE_6_1 |
| Use Case Name: | **Counselling** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel) |
| Description: | Get help and advice from school personnel.<br>Counselling can also be done in groups using restricting areas. |
| Trigger: | A pupil has requested counselling, or a member of staff has decided to set up a general counselling session aimed at a group of pupils. |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• The counsellor has started a counselling session.<br>• The user has proved he is a valid user of the system. |
| Normal Flow: | 1. The pupil navigates to the counselling section.<br>2. The system prompts the pupil to choose if the chat should be completely anonymously or partial by exposing some attributes. The pupil may also chat revealing her real identity.<br>3. The chat begins.<br>4. If the counsellor wants to verify the pupil's age or any other attribute, a request for the pupil's age (or other attribute) will be sent.<br>5. The pupil receives the request and can accept or decline the request.<br>6. If the pupil accepts the she uses her smart card to prove the requested attribute. |

## 3.9 Restricted Chat Room

| | |
|---|---|
| Use Case ID: | SE_6_2 |
| Use Case Name: | **Chat session in a restricted chat room** |

| | |
|---|---|
| Actors: | Pupils<br>Alternative actors can also be parents, school personnel. |
| Description: | This use-case describes two use-cases which are almost identical.<br>1. A person chats with other users by entering a chat room (group).<br>2. A person that wants to chat with another person in a private chat room (one-to-one).<br>Chat rooms = Restricted Areas with chat functionality activated |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• A restricted area with chat functionality has been previously created.<br>• The user has proved he is a valid user of the system. |
| Postconditions: | • Saved data will be encrypted if setting of RA is to encrypt and save.<br>• A history of all exchanged attributes during a communication session will be saved in the system. The next time the user access the same thread she will be notified of what information she exposed. |
| Normal Flow: | 1. The user navigates to the chat section of the website.<br>2. The system lists and groups of all public and available Restricted Areas that have chat rooms functionality activated. It also shows the access policy for each Restricted Area.<br>3. The user finds a chat room and clicks the join button.<br>4. The user goes through the use-case SE_6.<br>5. Upon success, the user can join the chat room.<br>6. The user is now able to send and read messages. |
| Alternative Flow: | |

| | |
|---|---|
| | A user (U1) wants to chat with another user (U2).<br>1. U1 clicks on U2 of a list of online users (U2 can be a real name or an alias).<br>2. If U2 has indicated in her profile that she can be contacted then U2 is informed that she has a communication request from U1.<br>3. U2 accepts the request.<br>4. A new RA with default settings is created by the system.<br>5. The RA has access policy that includes U1 and U2.<br>6. Both users will go through the use case SE_6.<br>7. A chat conversation can be conducted. |

## 3.10 Political Discussions

| | |
|---|---|
| Use Case ID: | SE_6_3 |
| Use Case Name: | **Political discussions (anonymous discussions)** |

| | |
|---|---|
| Actors: | Pupils<br>Alternative actors can also be parents, school personnel. |
| Description: | Political discussions are anonymous chats, with no option to reveal the identities. |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• A Restricted Area with chat of type political discussion has been previously created.<br>• The user has proved he is a valid user of the system. |
| Postconditions: | • The logs of the Restricted Area will be removed (deleted from the disk) unless the setting is to save the history.<br>• Saved data will be encrypted if setting of RA is to encrypt and save. |
| Normal Flow: | 1. Interested users navigate to the RA intended for the political discussion and click on the Join button.<br>2. The user goes through use case SE_6.<br>3. Upon success the user can join the RA.<br>4. The user is now able to participate in the political discussion by sending and reading messages into the chat, the forum etc. |

## 3.11 Sharing Documents

| | |
|---|---|
| Use Case ID: | SE_6_4 |
| Use Case Name: | **Sharing documents (grades and individual development plans)** |

| | |
|---|---|
| Actors: | Pupils, parents, school personnel. |
| Description: | The school is producing many documents (exam results, grades, individual development plans etc.) that need to be shared with or distributed to the pupil's and their parents. A personal Restricted Area exists for every user in the system. |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• The user has proved he is a valid user of the system. |
| Postconditions: | • The user gets access to the uploaded documents for her in the system. |
| Normal Flow: | 1. A user uploads a document to the personal RA of a desired user.<br>2. The user is notified of a new document in her personal RA.<br>3. The user navigates to the RA and click on the Join button.<br>4. The user goes through the use case SE_6.<br>5. Upon success the user can join the RA.<br>6. The user is now able to access and download the document. |

## 3.12 Polling

| | |
|---|---|
| Use Case ID: | SE_6_5 |
| Use Case Name: | **Polling (Optional)** |

| | |
|---|---|
| Actors: | Pupils<br>Alternative actors can also be parents, school personnel. |
| Description: | A poll in the fashion of "one question, multiple answers" is supported by the system. That is, the initiator of the poll can define a questionnaire with multiple answers where the users can select one or more answers, depending on the setting. (E.g., at the start of each semester each class needs to elect two class representatives.) |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the ‘User Agent App’ installed on it and a smartcard reader connected to it.<br>• A Restricted Area with polling functionality has previously been created.<br>• The user has proved he is a valid user of the system. |
| Postconditions: | • The user submits her opinion about the poll. |
| Normal Flow: | 1. Users navigate to the RA intended for polling and click the Join button.<br>2. The user goes through the use case SE_6.<br>3. Upon success the user can join the RA.<br>4. The user is now able to participate in the poll.<br>5. The pupil can update his answers until a given pre-defined deadline, when the polling ends.<br>6. After the end of the poll, the pupils are presented with the results. |

## 3.13 Revocation

| | |
|---|---|
| Use Case ID: | SE_7 |
| Use Case Name: | **Revoking a User's Credential** |

| | |
|---|---|
| Actors: | System Administrator<br>Revocation Requestor |
| Description: | A user's credentials can be made invalid. |
| Trigger: | • A user leaves the school or behaved repeatedly disturbing.<br>• The user (or her parents) revoke the consent and want to quit using the system.<br>• The attribute attested in an aux credential is no longer valid.<br>• There is no legal basis anymore for using the system.<br>• A user loses her SC or if the SC has been stolen. |
| Preconditions: | |
| Postconditions: | • The credential cannot be used to access any restricted area. |
| Normal Flow: | 1. A revocation requestor informs the System Administrator about the situation of a credential.<br>2. The System Administrator verifies the condition for revoking the credential.<br>3. The System Administrator commits the necessary information to the revocation authority. |

## 3.14 Emergency Situation

| | |
|---|---|
| Use Case ID: | SE_8 |
| Use Case Name: | **Emergency Situation (Inspection)** |

| | |
|---|---|
| Actors: | Inspection Requester (a user reporting the emergency situation)<br>Inspector(s).<br>Inspection Receiver |
| Description: | The inspector reveals the identity of a user |
| Trigger: | An emergency situation. |
| Preconditions: | • A user reports an emergency situation. |
| Postconditions: | • Some user's identity is revealed i.e. the encrypted attribute is decrypted. |
| Normal Flow: | 1. A user reports an emergency situation.<br>2. School personnel and other users responsible for triggering the inspector forward the relevant 'inspection data' to the inspector.<br>3. The inspector investigates the condition and checks if it is an emergency situation according to the policies.<br>4. If the inspector decides for revealing the identity of the user, the inspection data will be unfolded.<br>5. Inspection is securely protocoled / control person is informed (e.g. data protection official)<br>6. The inspector passes this information to authorized users<br>7. The authorized users must take appropriate actions<br>8. Depending on the situation, once appropriate, the user concerned will be informed that her identity has been revealed. |

## 3.15 Viewing/Deleting Credentials

| | |
|---|---|
| Use Case ID: | SE_9 |
| Use Case Name: | **Viewing/Deleting Credentials stored on the Smart Card** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel) |
| Description: | This use case describes the steps needed for a user to view/delete her credentials stored on her smartcard. |
| Preconditions: | • The user has initialized her SC or her PC (see SE_1).<br>• The user knows the credentials needed for accessing the smartcard contents (e.g. PIN).<br>• The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it. |
| Postconditions: | • All credentials and the attributes embedded into the credentials can be viewed/removed. |
| Normal Flow: | 1. User places her card on her smartcard reader.<br>2. The user starts the 'User Agent App'<br>3. The user selects 'View Credentials'/ 'Delete Credentials'<br>4. There 'User Agent App' asks the user to authenticate to the card.<br>5. The 'User Agent App' lists the credentials stored on the SC.<br>6. The user can delete each credential or get a human readable preview of its content. |

## 3.16 Changing PIN

| | |
|---|---|
| Use Case ID: | SE_11 |
| Use Case Name: | **Changing the Smart Card access credentials (e.g. PIN)** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel)<br>Inspector |
| Description: | This use case describes the steps needed for a user to change the access credentials of the Smart Card. |
| Preconditions: | • The user / inspector knows her old credentials<br>• The user / inspector has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it. |
| Postconditions: | The smartcard access credentials is changed |
| Normal Flow: | 1. User/Inspector places her card on her smart card reader.<br>2. The user/inspector starts the "User Agent App"<br>3. The user/inspector selects 'Change PIN' (The option will change if any other mechanism is used)<br>4. The user/inspector is requested to enter her old credentials (of the SC)<br>5. The "User Agent App" requests the user/inspector to enter the new credentials twice.<br>6. The "User/Inspector Agent App" checks the new values against a predefined policy,<br>7. The user/inspector will be informed if her smartcard access credentials has been successfully changed. |

## 3.17 Unlocking the SC

| | |
|---|---|
| Use Case ID: | SE_13 |
| Use Case Name: | **Unlocking the Smart Card with a PUK** |

| | |
|---|---|
| Actors: | Users (pupils, parents and school personnel)<br>Inspector |
| Description: | This use case describes how to unlock the Smart Card |
| Trigger: | The user/inspector fails 3 times in a row to properly authenticate to the smartcard. |
| Preconditions: | • The user has a PC with the 'User Agent App' installed on it and a smartcard reader connected to it.<br>• The user knows the PUK for unlocking the card. |
| Postconditions: | The SC is unlocked |
| Normal Flow: | 1. User/inspector places her card on her smart card reader.<br>2. The user/inspector starts the 'User Agent App'<br>3. The user/inspector selects 'Unlock SC with PUK'<br>4. The user/inspector is requested to enter her PUK (of the SC)<br>5. If the PUK is correct, the 'User/inspector Agent App' requests the user/inspector to enter the new smartcard access credential (e.g. PIN) twice.<br>6. The smartcard checks if the values are compatible with a predefined policy.<br>7. The user will be informed if the unblocking was successful. |
| Alternative Flow: | If the user/inspector entered 3 times in a row the wrong PUK (or if the user/inspector forgot her PUK) she must then contact the school administration to:<br>• Apply for a new SC<br>• Receive a new initial smartcard access credential (e.g. PIN) and PUK<br>• User only: Receive a new ID and a new OTP |

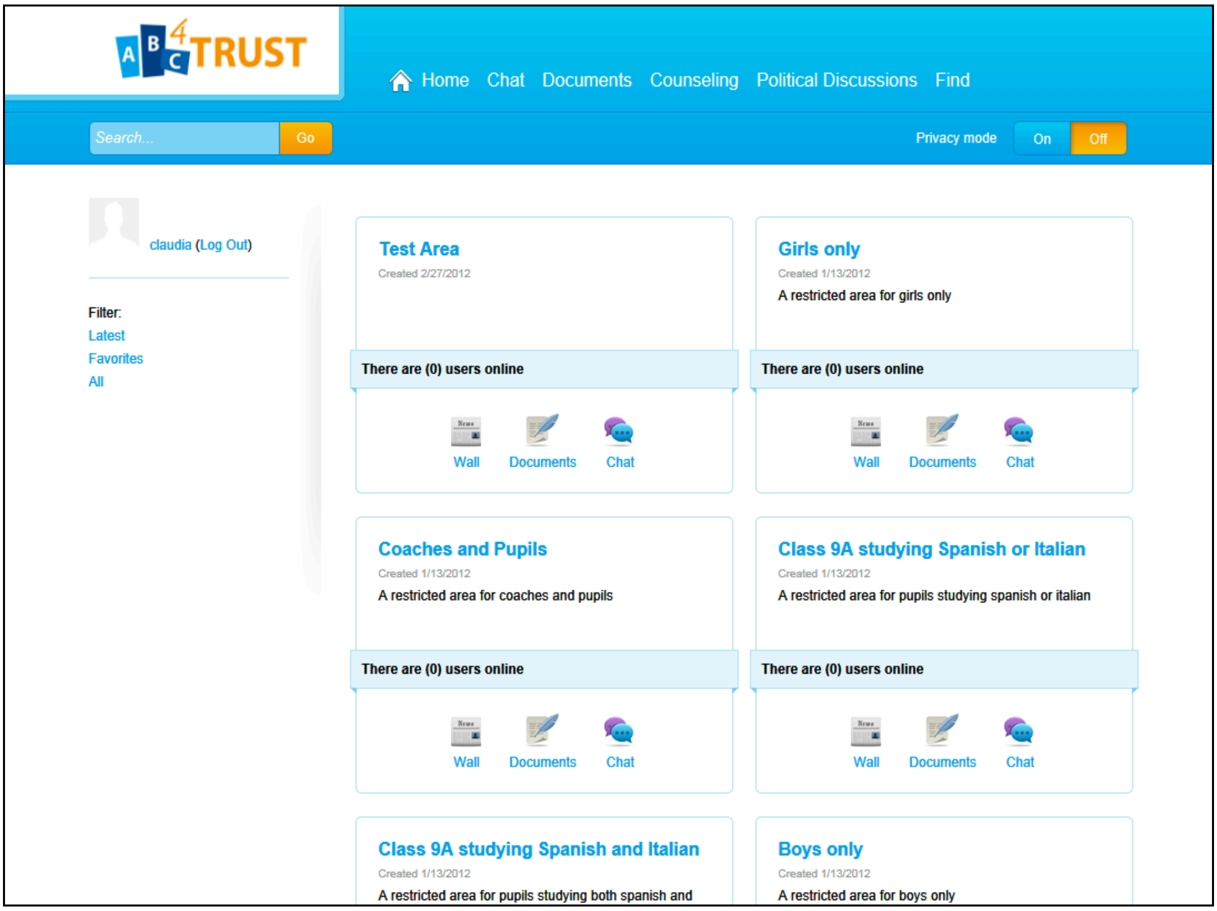
# 4 GUI Views

The GUI will use a simple, strict design. All of the school pilot's user interface should be functional in IE and Firefox browsers, and in general be in accordance with the HTML 4.1 standard.

The following GUI snapshots set the base for the design of the User and Admin sections of the Restricted Area system. The inspector and the revocation authority GUI will have a very simple layout and are not described in this document.

## 4.1 User GUI of Restricted Area

Figure 1 shows a list of available chat rooms. Each box shows some details about the chat room: Name, description, creation date and available functionality.



**Test Area**
Created 2/27/2012

There are (0) users online

**Girls only**
Created 1/13/2012
A restricted area for girls only

There are (0) users online

**Coaches and Pupils**
Created 1/13/2012
A restricted area for coaches and pupils

There are (0) users online

**Class 9A studying Spanish or Italian**
Created 1/13/2012
A restricted area for pupils studying spanish or italian

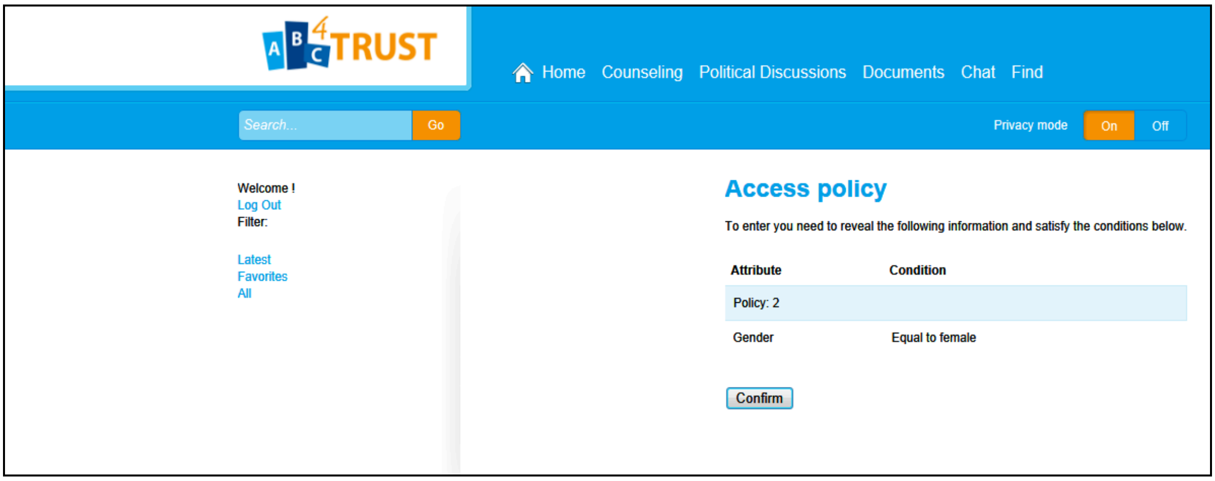
There are (0) users online

**Class 9A studying Spanish and Italian**
Created 1/13/2012
A restricted area for pupils studying both spanish and

**Boys only**
Created 1/13/2012
A restricted area for boys only

**Figure 1: School web application – List of available chat rooms**

Figure 2 shows what happens when a user tries to enter one restricted area by clicking anywhere in the box that contains the restricted area. The access policy and conditions that the user needs to meet in order to enter the restricted area are presented for the user. The user needs to confirm that he is willing to use his credentials and to prove to the system that he meets the access policy requirements. The system will compare the content of the users credential with the requirements defined in the access policy. In this case the user needs to prove that she is a girl and is willing to reveal this information about herself. No other information about the user will be revealed to the system.



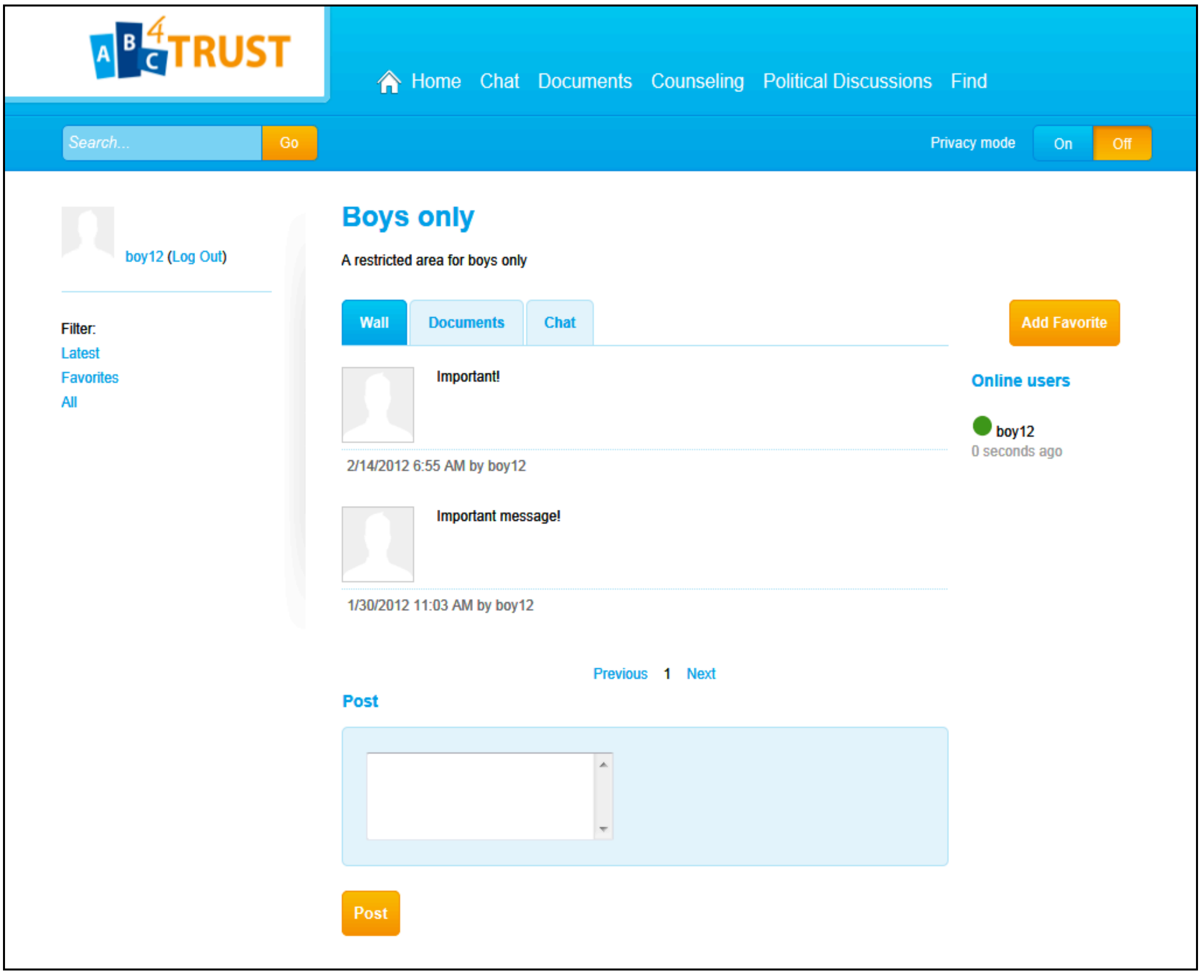
Access policy

To enter you need to reveal the following information and satisfy the conditions below.

| Attribute | Condition |
|---|---|
| Policy: 2 | |
| Gender | Equal to female |

**Figure 2: School web application – Access policy to meet**

Figure 3 shows a restricted area for boys that have the wall functionality activated. There are two messages in the wall.



Boys only

A restricted area for boys only

Important!

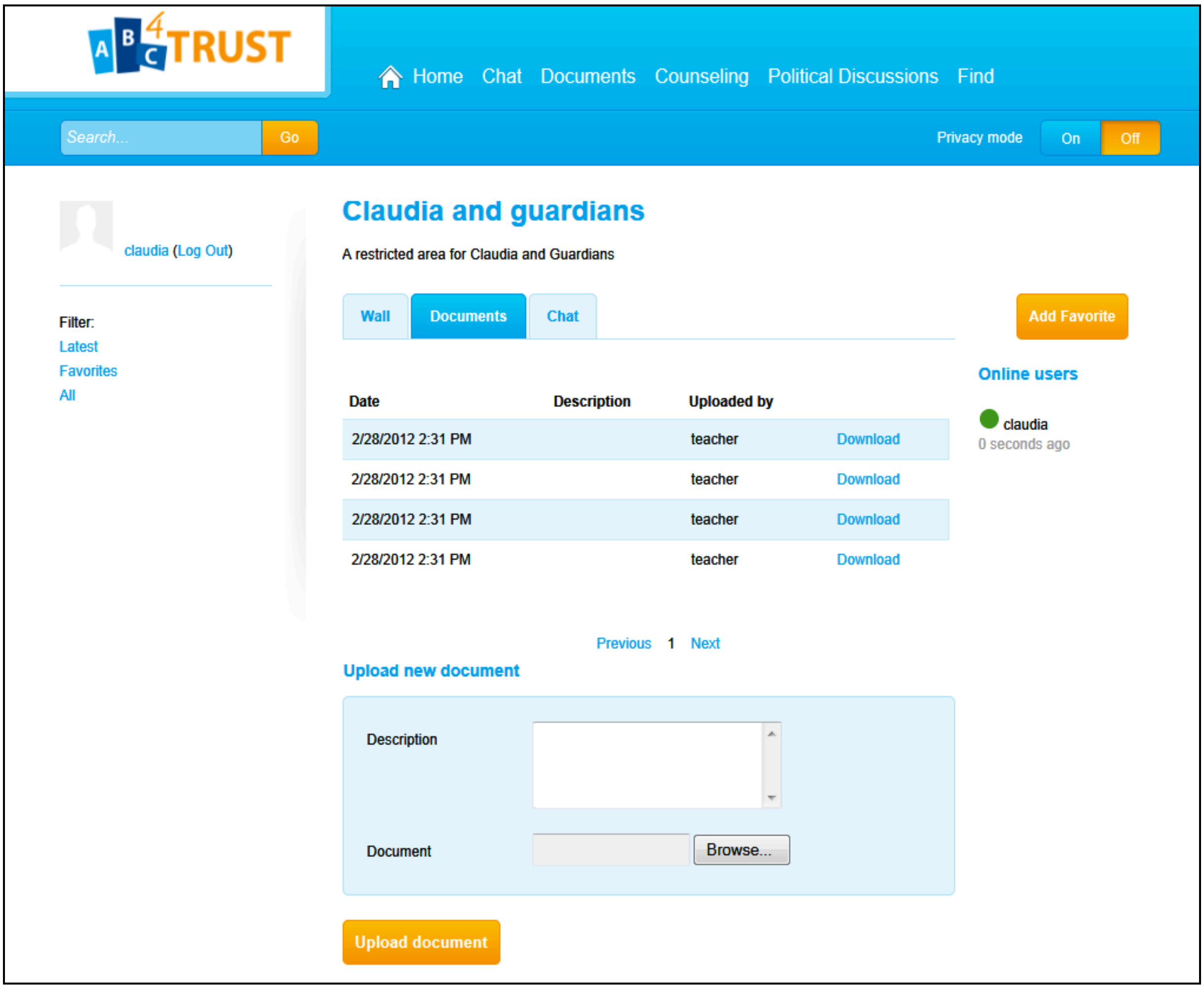
2/14/2012 6:55 AM by boy12

Important message!

1/30/2012 11:03 AM by boy12

**Figure 3: School web application – Wall**

Figure 4 shows a restricted area with access policies that includes Claudia and here guardians. The restricted area has the documents functionality activated and there are four documents uploaded to the area that can be downloaded by Claudia and her guardians.



Claudia and guardians

A restricted area for Claudia and Guardians

| Date | Description | Uploaded by | |
|---|---|---|---|
| 2/28/2012 2:31 PM | | teacher | Download |
| 2/28/2012 2:31 PM | | teacher | Download |
| 2/28/2012 2:31 PM | | teacher | Download |
| 2/28/2012 2:31 PM | | teacher | Download |

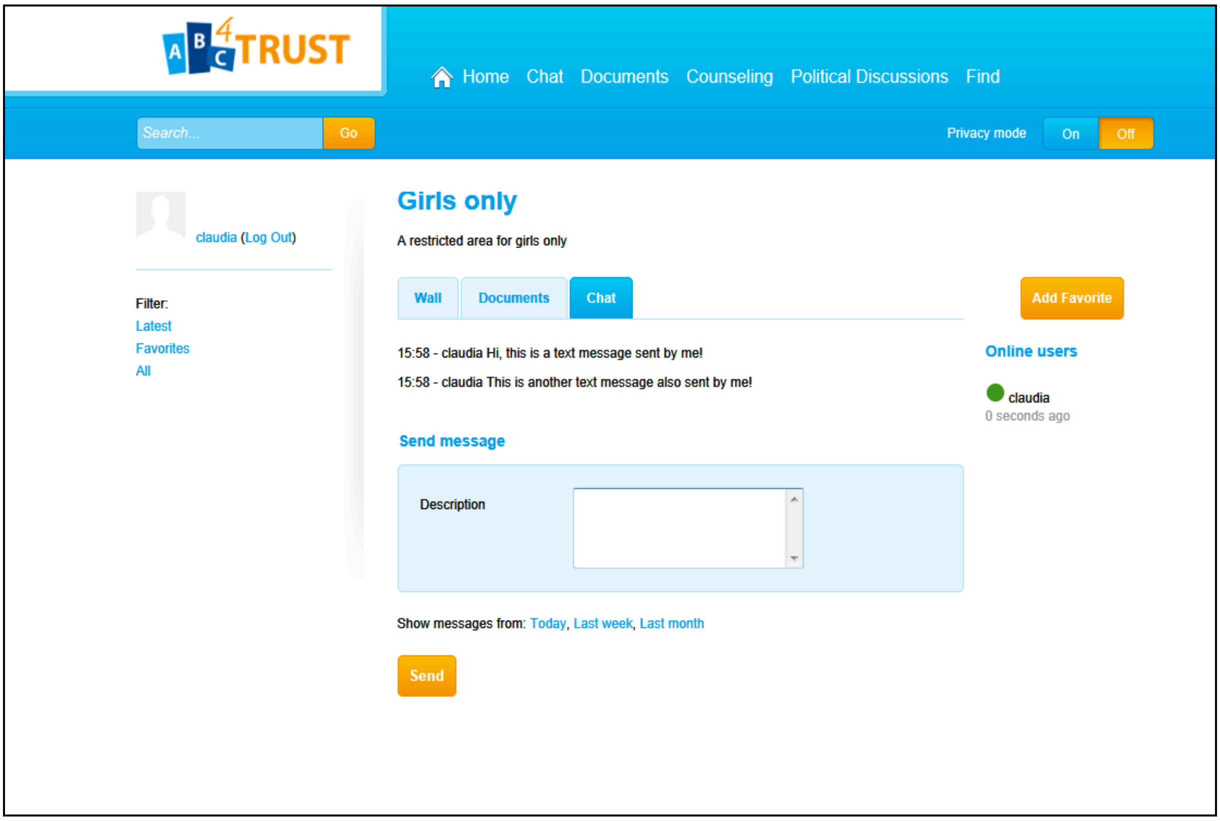
Upload new document

Description

Document

**Figure 4: School web application - Documents**

Figure 5 shows a restricted area with access policies that includes all girls. The restricted area has the chat functionality activated and there are two text messages that can be read by all other girls that can access the restricted area.



Girls only

A restricted area for girls only

15:58 - claudia Hi, this is a text message sent by me!

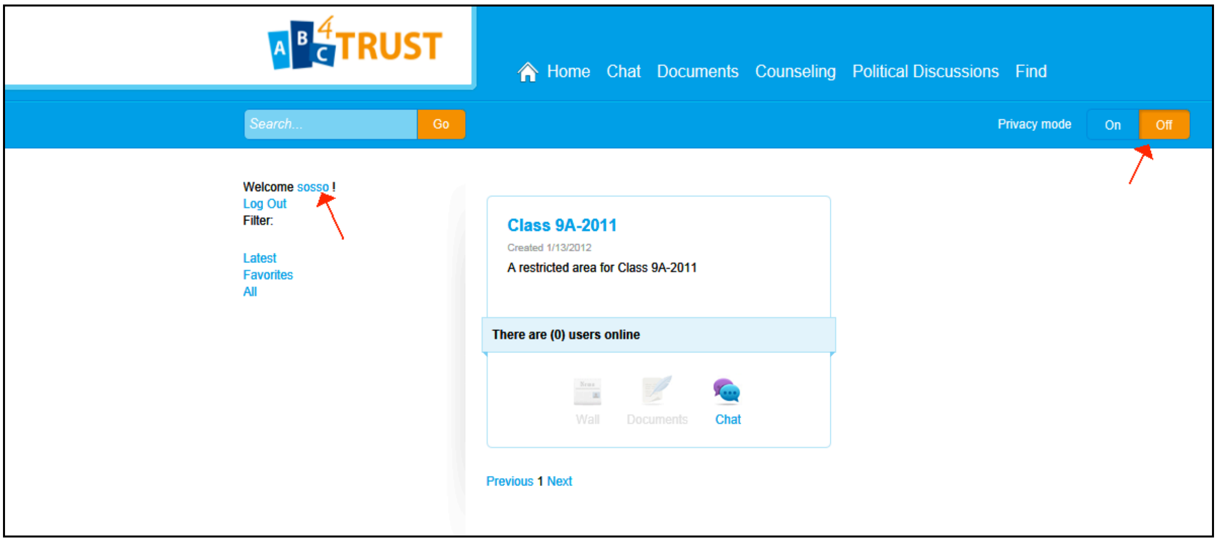
15:58 - claudia This is another text message also sent by me!

**Figure 5: School web application - Chat**

A view in secret situation occurs when another person is passing by, sitting beside or behind the user while using the web application. The person behind might be another pupil, a parent, a teacher or maybe a technical support person that is helping the user to use the system. No matter if it happens accidently or consciously, seeing what aliases, credentials, communication threads, messages or restricted areas are in use might reveal the anonymity the user and threatens his privacy.

To protect the user's privacy in these and similar situations the user can switch on his On-screen privacy mode.

Figure 6 shows how the screen looks like when the On-Screen privacy mode is "off". This means that information such as the name, the alias of the user, list of visited restricted areas and other sensitive information are shown on the screen. This functionality does not really use any complicated technical features but is privacy enhancing and in line with the intentions of the Privacy-ABC technology.



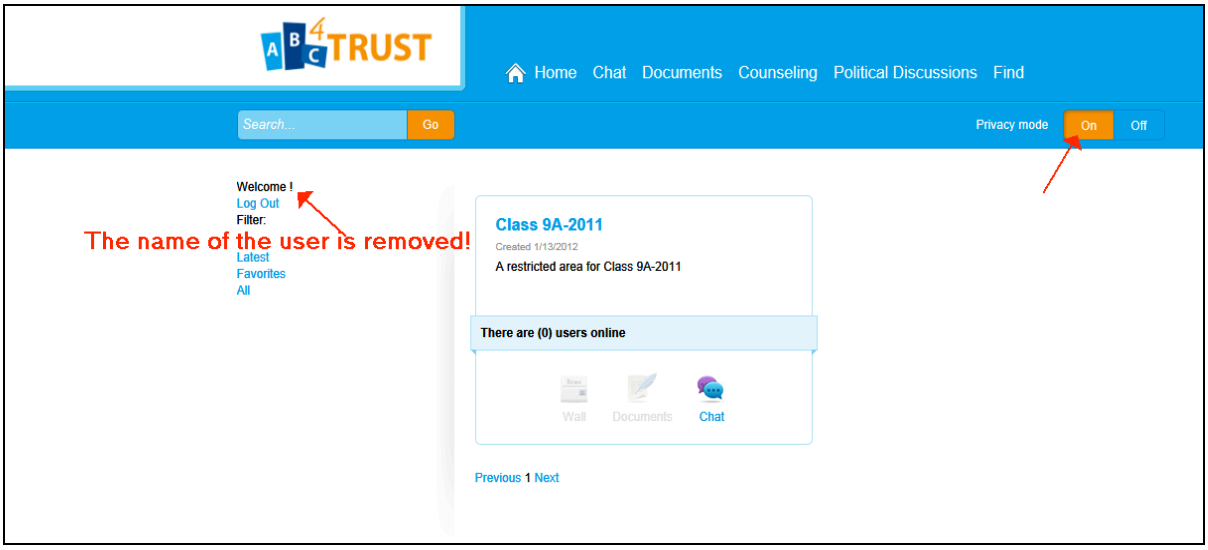
Welcome sosso !
Log Out
Filter:

Class 9A-2011
Created 1/13/2012
A restricted area for Class 9A-2011

There are (0) users online

**Figure 6: School web application – On-screen privacy mode is switched "Off"**

Figure 7 shows how the screen looks like when the On-Screen privacy mode is “on”. This means that information such as name of the user, visited restricted areas and other sensitive information are NOT shown on the screen.



The name of the user is removed!

Class 9A-2011

Created 1/13/2012

A restricted area for Class 9A-2011

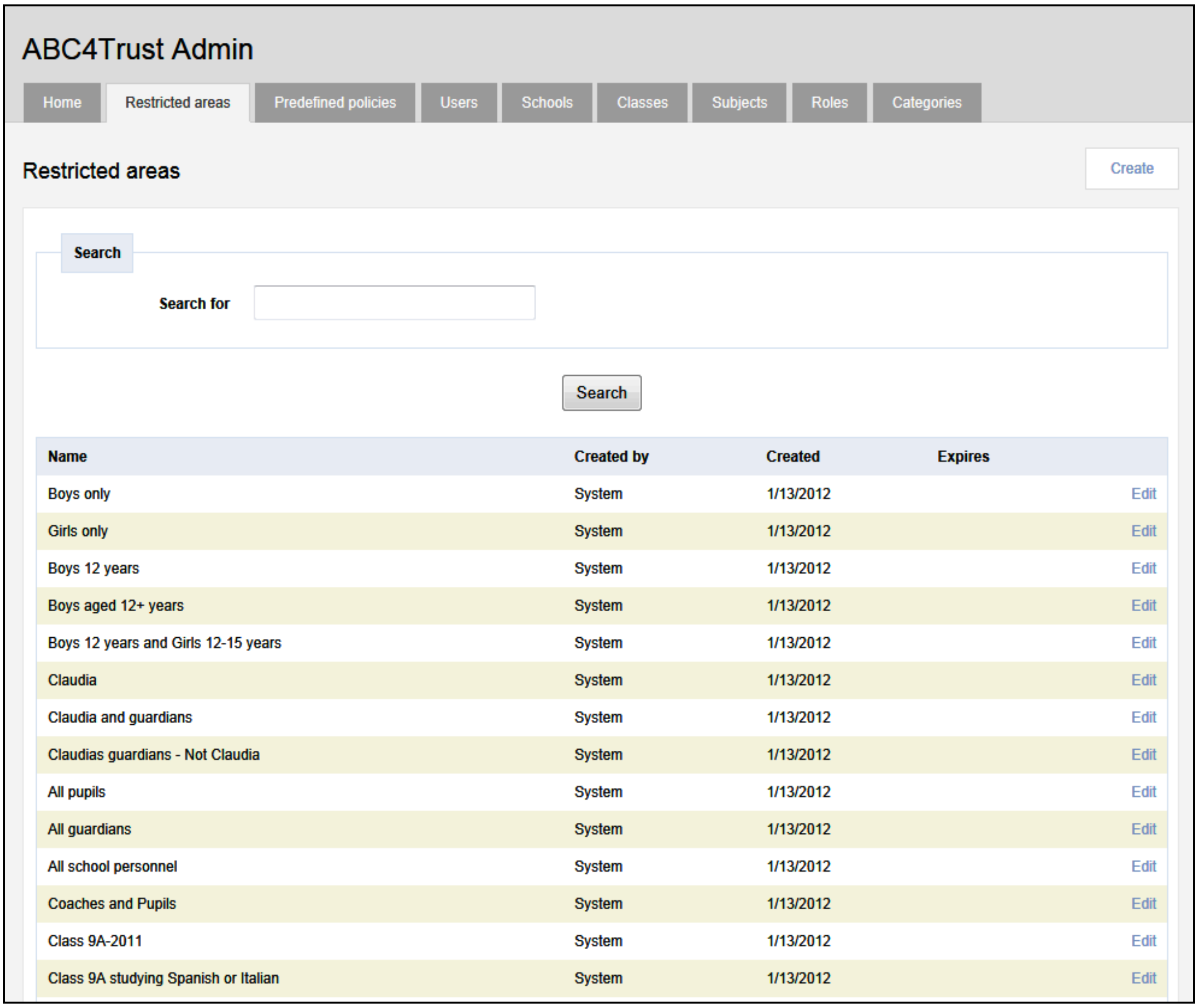
There are (0) users online

**Figure 7: School web application – On-screen privacy mode is switched ”On”**

## 4.2 Administration GUI of Restricted Areas

The following figures show some GUI from the administration section, where restricted areas can be created and defined.

Figure 8 shows a list of existing restricted areas. The administrator can add new restricted areas or edit and change any restricted area from the list and change its definition.



Restricted areas

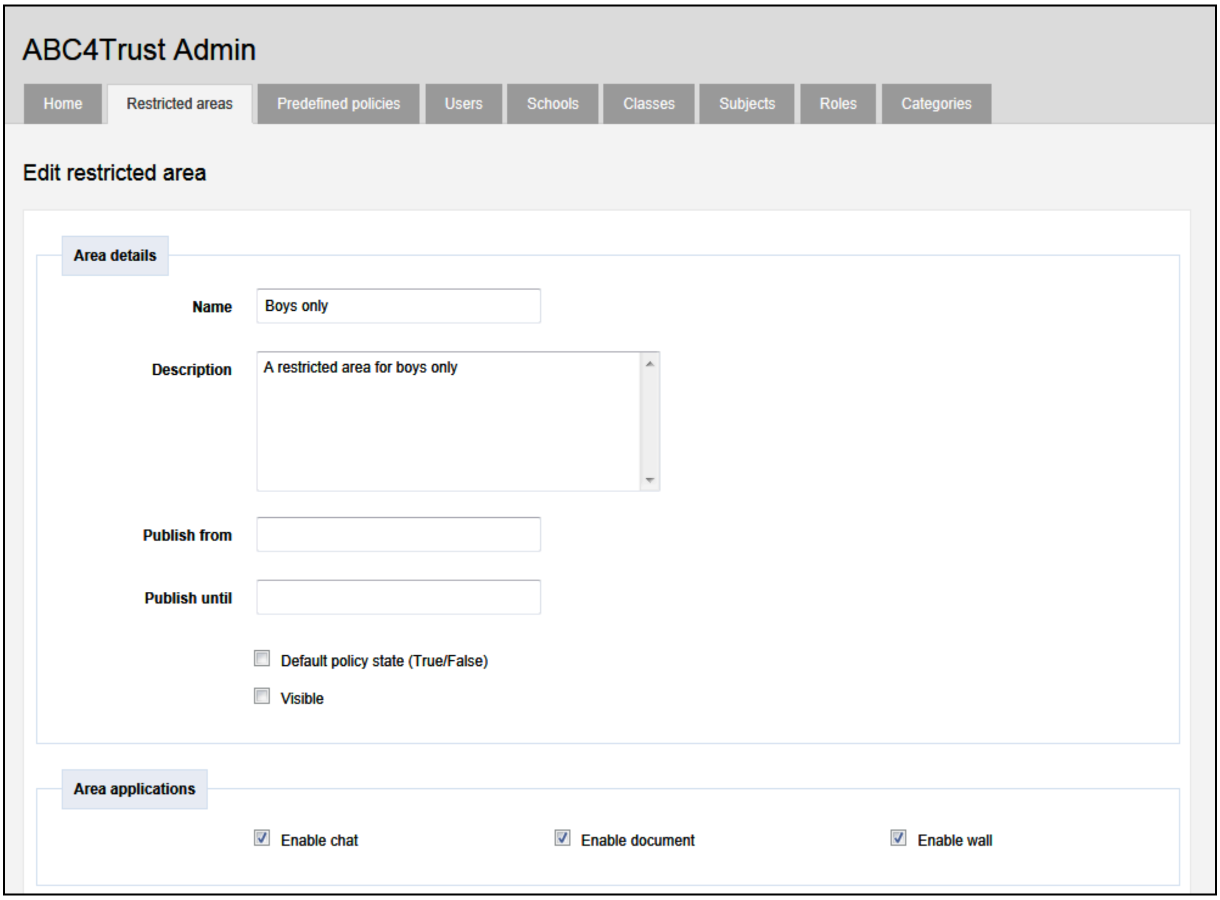
Search for

| Name | Created by | Created | Expires | |
|---|---|---|---|---|
| Boys only | System | 1/13/2012 | | Edit |
| Girls only | System | 1/13/2012 | | Edit |
| Boys 12 years | System | 1/13/2012 | | Edit |
| Boys aged 12+ years | System | 1/13/2012 | | Edit |
| Boys 12 years and Girls 12-15 years | System | 1/13/2012 | | Edit |
| Claudia | System | 1/13/2012 | | Edit |
| Claudia and guardians | System | 1/13/2012 | | Edit |
| Claudias guardians - Not Claudia | System | 1/13/2012 | | Edit |
| All pupils | System | 1/13/2012 | | Edit |
| All guardians | System | 1/13/2012 | | Edit |
| All school personnel | System | 1/13/2012 | | Edit |
| Coaches and Pupils | System | 1/13/2012 | | Edit |
| Class 9A-2011 | System | 1/13/2012 | | Edit |
| Class 9A studying Spanish or Italian | System | 1/13/2012 | | Edit |

**Figure 8: School web application - Administration section - List of Restricted Areas**

Figure 9 shows the editing and configuration of a Restricted Area details and Area applications (functionality). In this section authorized administrators allowed to create, edit and configure a Restricted Areas details.

- Name: Short name of the Restricted Area
- Description: A longer description of the Restricted Area
- Publish from: Starting date when the Restricted Area I accessible
- Publish until: Ending date, when the Restricted Area will not be accessible
- Area applications: Defining which functionality the Restricted Area will contain



Edit restricted area

Area details

Name: Boys only

Description: A restricted area for boys only

Publish from:

Publish until:

□ Default policy state (True/False)

□ Visible

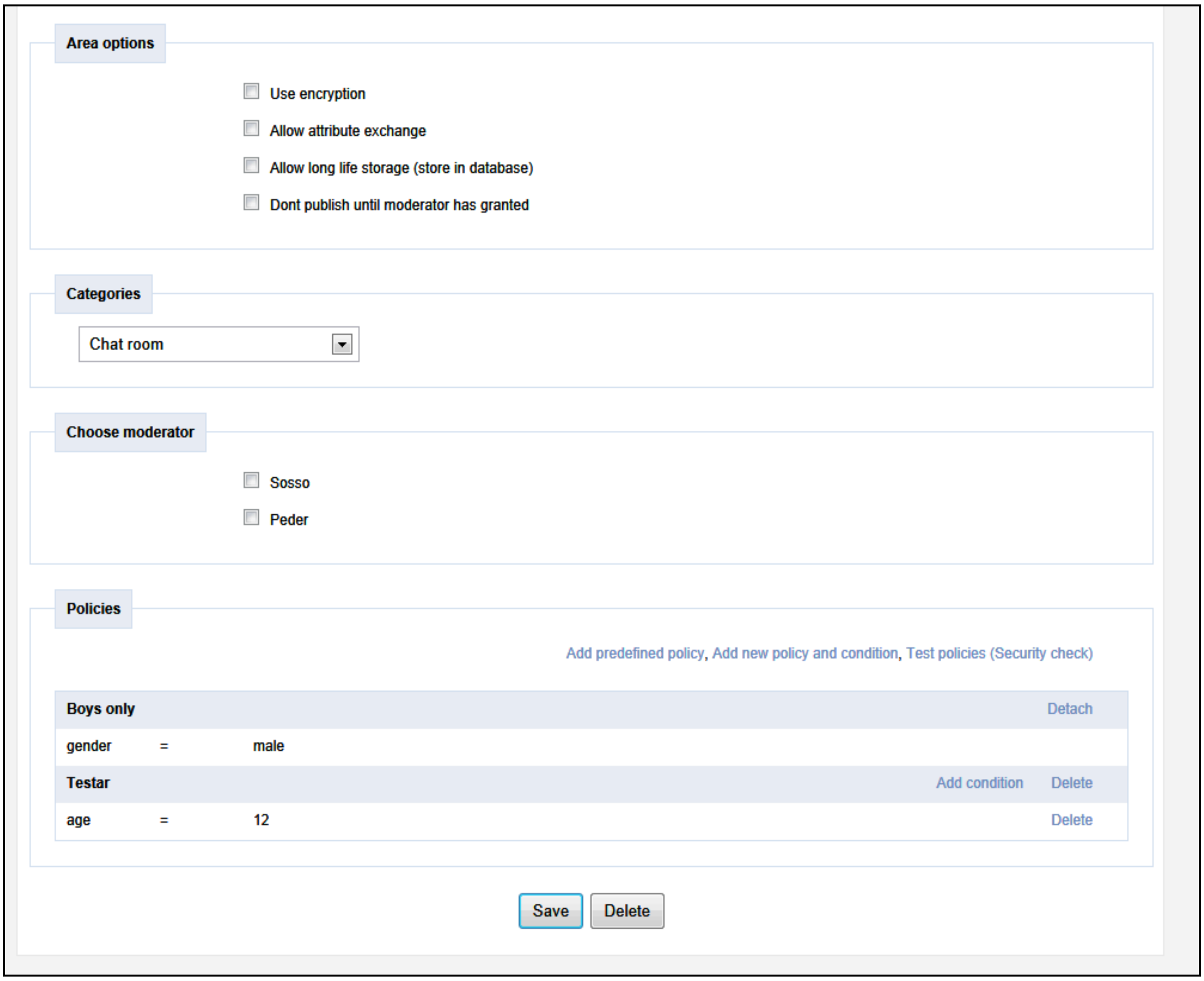
Area applications

☑ Enable chat ☑ Enable document ☑ Enable wall

**Figure 9: School web application - Administration section – Configuration of a Restricted Area details (part 1 of 2)**

Figure 10 (continuation of Figure 9) shows the editing and configuration of the following Restricted Area options:

- Use encryption: Communication will be protected by encryption (SSL etc.)
- Allow attribute exchange: Allowing or not allowing the users to exchange attribute in their communication
- Allow long life storage (store in database): Whether the data will be saved in the database or the data will be removed after a short time of period
- Don't publish until moderator has granted: This defines whether posted comments, conversations and documents need to be granted by the moderator before they are published
- Categories: This defines in which section of the portal a particular Restricted Area will be listed (Chat, political discussion, counselling or documents)
- Choose moderator: Here the administrator can add persons that will act as moderator and grant
- Policies: This section shows which access policies need to be met in order to get access to the Restricted Area



Area options

☐ Use encryption

☐ Allow attribute exchange

☐ Allow long life storage (store in database)

☐ Dont publish until moderator has granted

Categories

Chat room ▾

Choose moderator

☐ Sosso

☐ Peder

Policies

Add predefined policy, Add new policy and condition, Test policies (Security check)

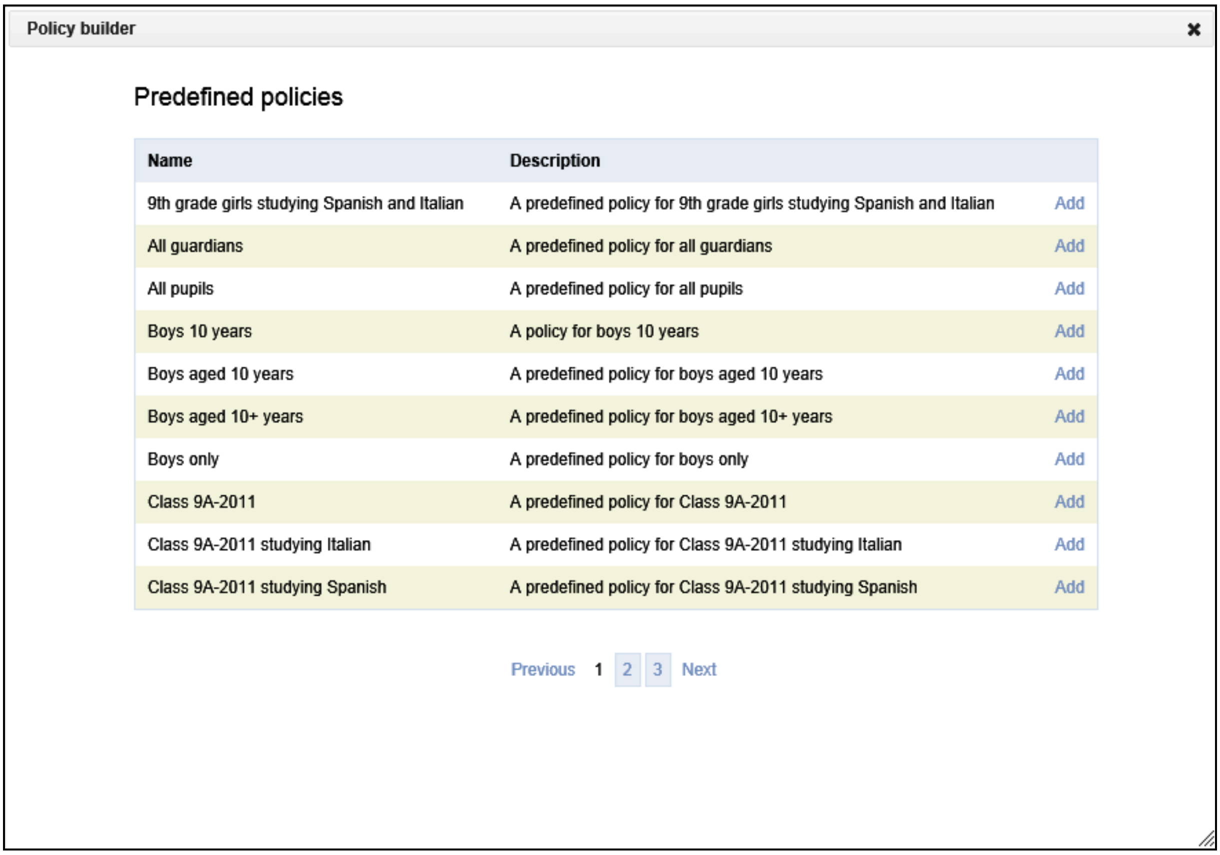
| | | | |
|---|---|---|---|
| **Boys only** | | | Detach |
| gender | = | male | |
| **Testar** | | | Add condition Delete |
| age | = | 12 | Delete |

**Figure 10: School web application - Administration section – Configuration of a Restricted Area details (part 2 of 2)**

### 4.2.1 Access policy builder

The following three figures show the access policy builder. The access policy builder section is where administrator can set up and configure the access policies defining who is eligible to access and enter a certain Restricted Area. This is done by either selecting an already existing predefined policy as shown in Figure 11 or by defining and adding a new access policy as shown in Figure 12. Creating and editing predefined access policies is shown in Figure 13.

Figure 11 shows a list of predefined policies that administrators conveniently can add to a restricted area. The reason for having predefined access policies is mainly for enhancing the user experience and make administration fast. The administrator is also free to create and define new access policies and conditions as shown in Figure 12.

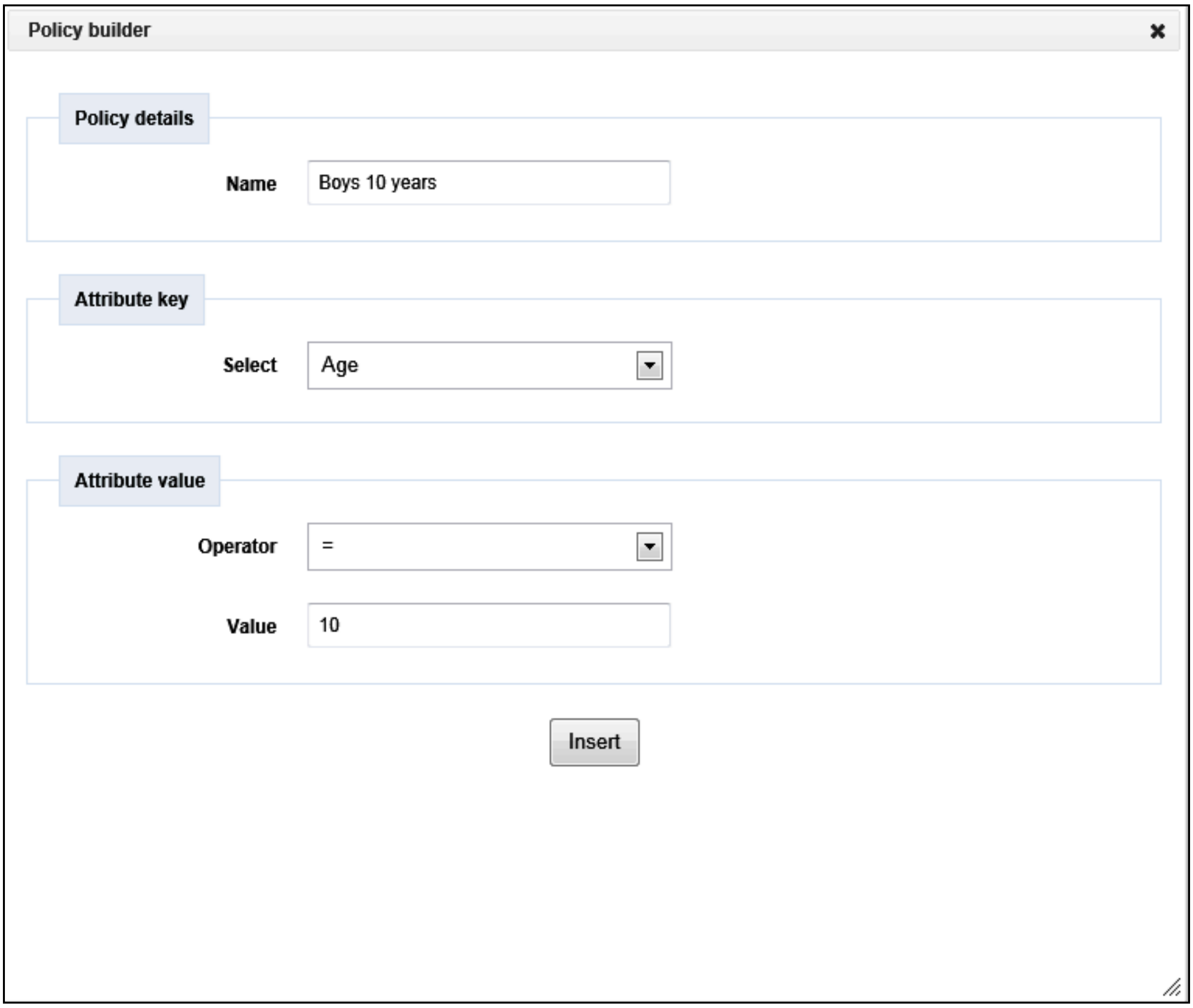


Predefined policies

| Name | Description | |
|---|---|---|
| 9th grade girls studying Spanish and Italian | A predefined policy for 9th grade girls studying Spanish and Italian | Add |
| All guardians | A predefined policy for all guardians | Add |
| All pupils | A predefined policy for all pupils | Add |
| Boys 10 years | A policy for boys 10 years | Add |
| Boys aged 10 years | A predefined policy for boys aged 10 years | Add |
| Boys aged 10+ years | A predefined policy for boys aged 10+ years | Add |
| Boys only | A predefined policy for boys only | Add |
| Class 9A-2011 | A predefined policy for Class 9A-2011 | Add |
| Class 9A-2011 studying Italian | A predefined policy for Class 9A-2011 studying Italian | Add |
| Class 9A-2011 studying Spanish | A predefined policy for Class 9A-2011 studying Spanish | Add |

**Figure 11: School web application - Administration section - Access Policy list**

Figure 12 shows the access policy builder where new access policies and conditions are created and defined. In this example the administrator is adding an access policy allowing 10 years old boys to enter the restricted area.



Policy details

Name: Boys 10 years

Attribute key

Select: Age

Attribute value

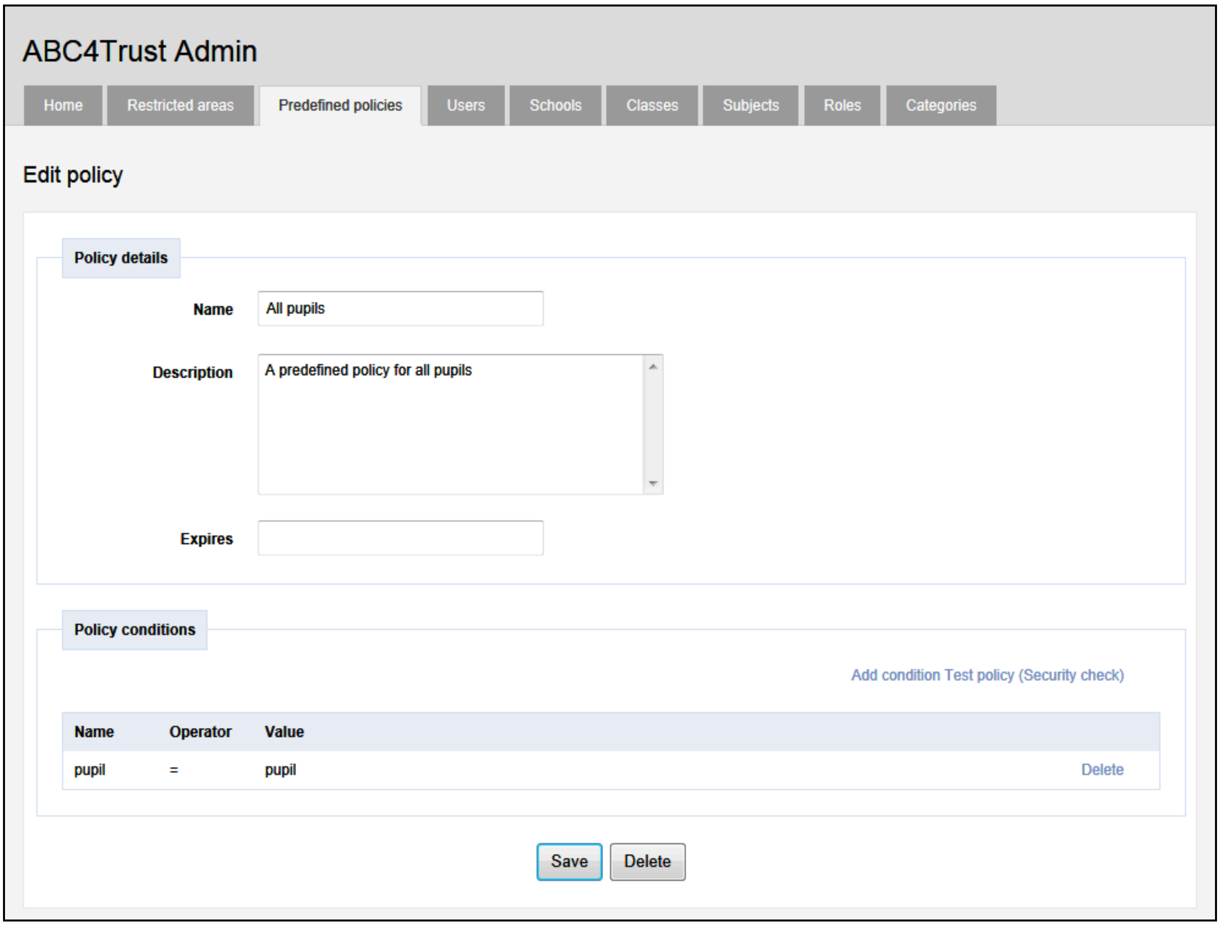
Operator: =

Value: 10

**Figure 12: School web application - Administration section - Access Policy Builder (building policy "boys 10 years")**

Figure 13 shows the access policy builder where predefined access policies are created and defined. Administrator will be able to create predefined system policies/conditions that can be used by all users. Predefined system policies will be created for the most common attributes and roles:

- Pupils
- Boys
- Girls
- Age 9
- Age 10
- Age 11
- …
- Age 16
- School personnel
- Guardians
- Class 7A-2013
- …



Edit policy

Policy details

Name: All pupils

Description: A predefined policy for all pupils

Expires:

Policy conditions

| Name | Operator | Value |
|---|---|---|
| pupil | = | pupil |

**Figure 13: School web application - Administration section – Configuration of predefined access policies**

# 5 Non-functional Requirements

## 5.1 System Requirements

Participants in the pilot are:

1. 400 pupils and their parents/guardians
2. 80 school personnel

All usage of the Restricted Area system will be through thin clients (web interface).

The administrator interface of the Restricted Area system will be used from Internet Explorer 8.

The user interface of the Restricted Area system has to cater to Firefox and Internet Explorer, preferably to allow usage of other web browsers too. It should adhere to W3C (draft) standards and provide valid HTML.

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

## 5.2 Defining security and data protection requirements via protection goals

In order to define the scope of the security and data protection aspects of the pilot, these aspects are briefly described in form of protection goals. This section does not state the comprehensive set of security requirements of the trial platforms. Instead, we focus on the security as well as the data protection specific goals that should be achieved.

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

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

> Confidentiality: Confidentiality is the requirement that information is disclosed only to authorised users of a system. It is the most common security requirement in all information systems expected to be satisfied for both stored and communicated information.
>
> Integrity: Integrity is the requirement that no unauthorised changes are made; both in data storage and in the transmission or that such change can at least be detected. For example, only authorised professors should be allowed to modify course material and grade.
>
> Availability: Availability is the requirement that authorised users can use a system when needed. Therefore, it should not be possible for usage of the system to be maliciously denied. For example, the course attendance application should not need interaction to the IDM system.

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

These data protection specific protection goals are explained as below:

> Unlinkability: "Unlinkability means that all data processing is operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy-relevant data outside of the domain, or at least that the implementation of such linking would require disproportionate efforts for the entity establishing such linkage. Unlinkability is the key element for data minimisation [PfiHan2010] because it encompasses all kinds of separating data from persons, e.g., by means of anonymization, pseudonymization, erasure or simply not having the data at all. In addition, it aims at separating different data sets, e.g., if they belong to different purposes, and thereby supports the principle of purpose binding. Further, separation of power is related to unlinkability. Unlinkability in this wide definition comprises the criteria from the Privacy Class in the Common Criteria (anonymity, pseudonymity, unlinkability (in a stricter definition), and even unobservability in the sense that any observation of another party cannot be linked to the action or non-action of a user). The overarching objective of this protection goal is to minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling spanning across contexts and thus potentially violating the purpose limitations related to the data." (cited from [ZwiHan2012])
>
> Transparency: "Transparency means that all parties involved in any privacy-relevant data processing can comprehend the legal, technical, and organisational conditions setting the scope for this processing – before, during and after the processing takes place. Examples for such a setting could be the comprehensibility of regulatory measures such as laws, contracts, or privacy policies, as well as the comprehensibility of used technologies, of organisational processes and responsibilities, of the data flow, data location, ways of transmission, further data recipients, and of potential risks to privacy. All these parties should know the risks and have sufficient information on potential countermeasures as well as on their usage and their limitations. This information should be given before the processing takes place (ex-ante transparency) which is in particular necessary if data subjects are being asked for consent or if data controllers want to decide on the usage of a specific system. But also subsequent to the processing, transparency on what exactly happened is important so that all parties can keep track of the actual processing (ex-post transparency)." (cited from [ZwiHan2012])
>
> Intervenability: "Intervenability means that the parties involved in any privacy-relevant data processing, including the individual whose personal data are processed, have the possibility to intervene, where necessary. The objective is to offer corrective measures and counterbalances in processes. For individuals, intervenability comprises the data subject's rights to rectification and erasure or the right to file a claim or to raise a dispute in order to achieve remedy when undesired effects have occurred. For data controllers, intervenability allows them to have efficient means to control their data processors as well as the respective IT systems to prevent undesired effects. Examples for such means may be the ability to stop a running process to avoid further harm or allow investigation, to ensure secure erasure of data including data items stored on backup media, and manually overruling of automated decisions or applying breaking glass policies." (cited from [ZwiHan2012])

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

By applying these protection goals to the setup of the pilot as it has been discussed and documented by now, a series of legal and other requirements has been derived. These are shown in the next subsection (see 5.3.)

## 5.3 Data protection and data security related requirements

This section lists the data protection and data security related requirements that have been identified for this pilot. This section is subject to minor changes and amendments as new challenges may be identified in course of the further development of the pilot.

### 5.3.1 Generic data protection requirements for the pilot

Some data protection requirements have been identified that relate to all use cases of the Söderhamn school pilot and will be reported in this section.

The goal of the ABC4Trust project is showing the advantages of Privacy-ABCs as method for authentication. From the view of the data protection law, Privacy-ABCs have three central advantages (see [KLNPZ11], p. 70 et seq.): First, Privacy-ABCs allow authenticating only with the attributes that are actually necessary to be processed for the purpose pursued by the data controller (selective disclosure). Second, if Privacy-ABCs are used to authenticate towards different services or for several access attempts, such actions remain unlinkable among each other, unless linkability is expressly required. Third, in case that personal data is only necessary under certain conditions, such as an emergency or extreme mobbing, the optional inspection functionality allows having a trusted entity retrieve the identifying attributes – a feature that could overcome concerns of, e.g., businesses and other stakeholders against the privacy preserving technology. To preserve these advantages, the following requirements should be fulfilled throughout the pilot:

- Guiding principle of the pilot shall be data minimisation, namely processing only the personal data which is necessary for archiving a given purpose.
- Methods for tracking or identifying Users such as IP logging, use of cookies or traffic analysis must not be used. In course of a pilot within a research project such as ABC4Trust, it might not be possible to address all such potential threats. In this case, the users should be pointed to it as part of the educational aspect, e.g. for anonymizing IP-addresses users could be pointed to the existing onion routing services.1 Ideally, the pilot deploys some safeguards on the network communication layer to secure Users from traffic analysis, IP logging etc.
- Where linkability is required for a particular service, this must not be done on the service side but rather with the means provided by the ABC-technology or e.g. with a user-centric approach, storing the necessary information under the control of the user. E.g. storing the information about visited restricted areas on the smart card, which is under the control of the User.
- Users must be enabled to ensure that no more personal data than required to prove their access rights will be disclosed to the system. For this, Users require knowledge of purpose and the defined access criteria.

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

- To prevent impersonation, the system must be capable of preventing access with lost smart cards or compromised credentials once a notification has been given, e.g., by revoking credentials.
- The inspection feature must be used reluctantly and remain the exception to the rule that Users remain anonymous and exclusively authenticate with the necessary non-identifying attributes.

The project's pilot deploying Privacy-ABCs must be legally compliant with data protection law and other applicable national legislation. Preferably, some of the data security and data protection goals should in parts exceed the legal minimum requirements– seen in comparison to widely used authorisation methods.

- Data subject's rights, such as the right of access and rectification, must not be unduly limited. Instead, the realisation of data subject's rights should be pursued to the greatest possible extent.
- According to the transparency principles, the User should be informed about who is processing which personal data for which purposes. Privacy-ABCs can be a major enabler for transparency as the GUI necessarily consists of a screen for attribute selection where the User can assemble the data to be sent. Also the necessary information about the receiving party can be displayed.
- Confidentiality: Personal data must only be accessible for entitled entities. Unusual access and processing should be made known to the data subject.
- Transparency requirements must be met, meaning that participants are enabled to learn to know who processes which personal data for which purpose. Possible measures to reach this goal include documentation, e.g., with:
    - Privacy and Security Policy including a description of the personal data processed and the purposes, the identity of the responsible data controller and involved data processors,
    - Description of the architecture and the data flows,
    - Contact details of the helpdesk or other persons than can help with problems,
    - Contact details for the revocation authority.
- For all data processed or stored, a clear and unambiguous deletion date must be specified depending on the type of data and purposes. As far as some statistic analysis is necessary for the evaluation of the pilot the storage period of the User's data must not exceed 6 months after the end of the pilot trail and should be limited to 3 month where possible.
- Prior to the trail, the retention period will be fixed and communicated as part of the privacy policy.
- Personal data must not leave the smart card without the explicit consent of the user, e.g. secured with a PIN.
- The secret key stored in the smart card must not leave the smart card and the end user should be involved in the key generation phase.

Special consideration must be given to the circumstance that the majority of the participants are minors. With pupils as target group, some special consideration must be given to their needs as well as regarding their legal guardians (usually the child's parents).

- Legal basis: A consent given by minors might require involvement of the legal guardians. The guiding legal principle is the “best interest of the child”, see Art. 3 para. 1 of the United Nation Convention on the Rights of the Child.2 It is accepted that children have a right of participation in decisions related to their right of privacy including making own decisions according to their level of physical and psychological development ([Art29WP160], p. 5 et seq.). Pupils must declare their consent personally and may withdraw it anytime.
- Legal guardians need to declare their own consent for their personal participation.
- For legal certainty the legal guardians need to sign their child’s consent form, too.
- Pupils becoming of age during the trail. A special problem might be caused by pupils turning 18 years in the course of the trail as this raises questions as to how a previously given consent from parents should be treated. While already the selection of the target group should exclude this event, ABC4Trust will always respect the rejection of giving consent or a later withdrawal of a consent by either the child or a guardian.
- Descriptions of how the personal data of the participants will be processed should be available in an age-appropriate form. Explanations including a version of the privacy policy need to be understandable for the pupils. However, such a version does not need to be comprehensive. Rather a special version covering the essentials should be provided in addition to a full and comprehensive privacy policy.
- The system must not allow guardians to view what their children have written without knowledge of their children. E.g. access is only possible with the smartcard and PIN of the children.

### 5.3.2 Use case specific data protection requirements

Several requirements are specific to use cases and will be discussed in relation to the respective use case. For details on the use cases, please refer to section 3.2 above.

#### 5.3.2.1 Obtaining a School credential from the School Registration Service

Before the participants can actually retrieve a credential from the School Registration System, its IdM database needs to be initialised with the participant’s data. For running the School IdM system, the school is the responsible data controller. EDOC will operate the necessary systems on behalf of the school as a data processor. NSN is another data processor taking care of the technical aspects of the IdM System.

Requirements related to the setup of the system and issuance of process:

- The transmission of the personal data of the participants (pupils and staff) to the database of the test system requires a legal base. In absence of a specific legal permission this needs to be covered by the informed consent.
- The content of the IdM database must not be accessible for unauthorised entities.
- Changes to personal data in the IdM application must only be possible for accredited persons. Any authorised changes must be traceable.
- To prevent impersonation or attempts to deceive other participants about untrue attributes only authorised entities are allowed to retrieve a credSchool. Planned measure: Login with a one-time password.

[2] Available online: http://www2.ohchr.org/english/law/crc.htm

- Availability: The School Registration System with its components plays an essential role for the role out of the pilot. It must be available until all participants have collected their credSchool. For obtaining additional credentials, a lower level of availability is acceptable.
- Methods for temporarily (re-)identifying a User may be used for the IdM system if this adds to security and/or usability of the system. E.g. a session cookie and/or storing the IP-addresses for the duration of the connection to prevent that a session gets taken over by a third person.

Requirements related to the involvement of data processor and / or remote access:

- Data processing requires a written contract between the data controller and the data processors. Details such as technical and organisational measures to ensure data security and data protection must be internally documented.
- The IdM database is physically located in Sweden. Remote access for administrators located at NSN in Munich must be possible.
- Access by data processors to the database with the participant's data should be traceable for the data controller. Plausibility checks regarding the necessity of the access will be done in regular intervals.
- Fine-grained access controls to the administrative section of the IdM system is required, including matching access authorisation schemes.
- Reasonable technical and organisational measures to protect personal data in the School Registration System must be taken. These will serve general data security as well as specifically personal data protection purposes. Generally, access to the personal data of test participants for NSN should be strictly limited to the extent absolutely necessary. During the further project runtime, organisational and technical measures will be identified in cooperation with all involved partners. Examples for such measures are:
  - Logging of remote accesses or automated messages to the responsible entity (school administration).
  - For the remote access: NSN is having its seat in Munich, Germany. Thus, any flow of personal data would include a cross-border transmission of personal data. Preferably, the maintenance of the IdM system should take place without granting any access to participant data. Where such access is necessary, double-check procedures should be established, e.g., by having a Swedish representative watch the access on-screen in real time.

#### 5.3.2.2 Viewing of the User's Data in the IdM Database and Self-Administration of the User's Data in the IdM Database

The participants have a right to access and, where necessary and possible, rectify personal data according to Art. 12 of Directive 95/46/EC, or accordingly to Sections 26 and 28 of the Swedish Personal Data Act (1998:204).[3]

- Only the authorised User may gain access to her personal data for viewing.
- In case of minors also the legal guardians may execute the right of access on behalf of the children. This may require the assistance of the data subject (the child).
- The User should be given access right to the personal information herself stored within the IdM system. Where appropriate, the user should be able to rectify her personal data herself.

[3] Available online: http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/

This is an optional use case as so far credSchool does not contain self-chosen attributes tending to change during the duration of the trail.

- In case of errors, the school as responsible data controller corrects the data upon request of a participant. This could trigger the need to issue a new credential.

#### 5.3.2.3 Common requirements for all restricted areas

The Restricted Area System provides the participants with containers that can hold several types of services including direct chat between two individuals, group chats, fora polls or specific counselling sessions. The areas share a set of requirements:

- Accessing or instantiating a restricted area must not be linkable to the accessing other restricted areas on the system, unless clearly identifying information has been used.
- Access to restricted areas is limited to Users that have proven to fulfil the published access criteria.
- Access to the content of restricted areas must be blocked or limited also for administrators of the restricted area system. Access of administrators must be stored in protocols.
- The User may access/manage several areas with her own access rights.
- By default inspection is deactivated in restricted areas.
- Users are allowed to use self chosen alias names (screen name used as a pseudonym).
- An alias name may only be claimed once.
- Users should be able to continue their previous postings or sessions once they authenticated for the previously used alias.
- Impersonating an alias should be prevented. Preferably, an alias is transferable, e.g. to be used by a group of people or a proxy.
- Users should be able to delete their messages posted under their alias. The system must indicate that messages have been edited or removed.
- A user initiated deletion must have the immediate effect that the respective content will not be shown to other persons viewing the restricted area. For the physical deletion of such content an appropriate deletion period must be fixed respecting the rights of the User and possible conflicting rights of third parties.
- Optional: Before accessing or instantiating a restricted area, it the GUI should indicate whether the chosen combination of attributes allows an identification of the User and/or provides the estimated size of the anonymity set. For this purpose, access of the restricted area system to the personal data on the School Registration Service is not permitted.
- Users should be able to easily find the restricted areas they have used lately. Such information allowing profiling the users behaviour must not be stored centrally but under the control of the user.
- The user must be able to create local backups of central information, e.g., on previously visited restricted areas.

#### 5.3.2.4 Instantiating (=creating) a Restricted Area

For the pilot, a series of restricted areas will be provided by the school. Users are also allowed to instantiate own restricted areas. For this case some requirements need to be met:

- The User instantiating may freely set access criteria that can be proven with the existing attributes on cards.
- The User instantiating a restricted area should be able to fulfil the access criteria herself.
- Before instantiating or accessing, the GUI views the necessary attributes.
- If an inspection is foreseen to eventually reveal the identity of a guest or host in a restricted area, Users must be informed in advance before entering the area including information about the inspection grounds and the identity of inspectors.

#### 5.3.2.5 Counselling session in a restricted area

During counselling, special categories of data may be exchanged in particular related to racial or ethnic origin, religious or philosophical beliefs, health and sex life. On the side of the Counsellor, further specific duties resulting from professional secrecy may apply.

As in the counselling cases, inspection will be enabled allowing identification of a User in case of an emergency, e.g. a suicide threat counselling cannot be treated as anonymous. Even if the User does not authenticate with identifying information towards the restricted area system, linking the conversation to the user is still possible via the inspection process.

- Where applicable, for particular for Counsellors, rules of professional secrecy must be obeyed.
- By default, counselling sessions are on a 1:1 basis. A third person may only be invited with consent of the pupil.
- Users must be informed in advance before entering the area including information about the potential inspection grounds.
- Counsellors authenticate with their particular qualification. Usually, a Counsellor should be identified with name and qualification.
- In case of an inspection, the Counsellor must participate, e.g. at least act as the inspection requestor.
- An affected User must be informed about an inspection as timely as possible and reasonable.
- The content of counselling sessions must be kept secret from third parties. The storage period on the restricted area system should be kept as short as possible. The User and/or the counsellor may have the possibility to keep a local copy. The counsellor must take appropriate measures for data security, e.g., encrypted storage.
- The pupil should be able to store a local copy of the content of a counselling session.
- Alias names used for counselling should not be used for other purposes within the system.

#### 5.3.2.6 Chat session in a restricted area

Chat sessions can be on a one to one basis or with several participants. Participants can either be identified or access with proving the required attributes only.

- The exchanged message in a private chat (one to one) should not be visible to anyone else than those two parties (even to the system administrators).
- The deletion period for chats should be chosen as short as possible.
- In private chats, each of the partners should have the possibility to trigger an immediate deletion of the whole conversation from the restricted area system once the chat has ended.
- The content of chat sessions should only be visible to the persons that are currently online. Persons joining start reading the moment they join.

- All current chat users are indicated to all other chat partners (list of alias names).

#### 5.3.2.7 Sharing documents in a restricted area

Restricted areas may be used to store and share files among participants. Each student gets a personalised restricted area which can store communication with the school also targeted for the parents. Besides the generic requirements, which are valid for all restricted areas such as allowing access of authorised Users only, no special security or data protection related requirements apply.

#### 5.3.2.8 Polling in a restricted area

For polling an election, a generally high level of trust is required in the system setup. To allow participation and inclusion of all pupils, the polling must not be used if one pupil does not participate in the trail and should not be used if a person concerned objects to the electronic form of polling.

#### 5.3.2.9 Revoking a User's Credential

If a pupil looses her smart card, leaves the school, withdraws the consent to participate or other reasons for excluding her from the trail occur the following requirements must be met:

- A procedure must be set up to prevent that a  User gets impersonated or a credential can be Used to authenticate towards the system after an incident has been reported. This service needs to be available and react within an appropriate timeframe.
- The User's personal data must be deleted from the IdM system in due time after the participant left the trial.
- It must not be possible to use the User's credentials or smartcard to impersonate the User or to access her data.
- The User should have the possibility to retrieve her data from the system, e.g., delete personal data copy scholastic information and input provided.
- Pupils/parents will be informed about storage durations and dates/cases of personal data deletion.
- Where permissible Users should still have deletion/correction access to data they have contributed to the system.

#### 5.3.2.10 Emergency Situation (Inspection)

A clear workflow for the handling of the emergency case must be defined. This entails the following aspects:

- Setting preconditions for the emergency situation. This entails a pre-definition of emergency needs (e. g. protection from immediate danger for life or health, amok, etc.). Such emergency triggers should be as detailed as possible. However, where generic permissions are required by law, the pre-definition may remain on a high level, but must refer to the legal conditions (court warrant or written statement of criminal prosecution authority, demanding the identity of one or more Users of a specific restricted area).
- Accessibility of these preconditions through contractual relationship in advance. The conditions should be public for the Users of the system and visible to all persons affected.
- Determination of a User notification policy. A User must be informed about the inspection by the inspector as soon as the circumstances permit it.
- Secure logging and documentation of any inspection process for later analysis.

- The emergency handling should be reviewed by a predefined control organ. E.g. by having a third person verify the necessity ex post, or by defining a double-check procedure with more than one inspector (or inspector and counsellor) required to reveal the identity.

#### 5.3.2.11 Viewing and Deleting Credentials stored on the Smart Card or on the PC

The participants have the data subject's right to access and rectification of personal data according to Art. 12 of Directive 95/46/EC, or according to Sections 26 and 28 of the Swedish Personal Data Act (1998:204).[4] This is not only valid for personal data under the control of a third person (IdM system, see above), but also for data under the physical control of the User herself, and thus applies to the data stored on the smartcards.

- The User must be given access rights to the content of her smartcard.
- In case some data is excluded from access, this must be known to the user, e.g., the User's Secret as a feature provided by the Smart Card cannot be accessed for security reasons.

Where appropriate, the user should be able to rectify her data herself. While this might be difficult for credentials it may be possible for the file storing the information on visited restricted areas.

## 5.4 Volume and Performance Expectations

The total number of users (all types) is estimated to 1300 in the school pilot.

The total number of smart card readers used in the school pilot will be approximately 1080.

The Restricted Area system needs to be able to cater to 300 concurrent users.

The Restricted Area system needs to be able to handle 2500 RAs.

The maximum tolerated response time of the Restricted Area System is two (2) seconds from the server.

## 5.5 Other Non-functional Requirements

1. Graphically prepared SCs are necessary showing amongst others the name of the authorized user. Graphical finalization must be done by School personnel, therefore the school must be provided with two card printers.
2. A small set of Users must be able to participate in the Söderhamn Pilot without smart cards. The credentials and certificates will then be stored in a secure area of the PC or laptop.
3. The School Administration System must contain a minimal subset of certified attributes for the students
4. A user can have multiple credRole, credGuardian, credChild, credClass and credSubject Privacy-ABCs
5. Every user will have at least one credRole credential.
6. 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.

[4] Available online: http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/

7. 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.
8. 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.
9. 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.
10. Informed consent required by pupils and parents before the processing of personal data begins.
11. Age of the pupils and capability of comprehension must be considered for user interfaces as well as for legal and information material
12. An optional date of expiry of Privacy-ABCs (e.g. for credSubject) must be supported

## 5.6 Credentials

**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'.

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 the attributes have been distributed 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.

***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

***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.

***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’.

***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’ , ‘Nurse’, ‘Teacher’, etc.

***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’

***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’

**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 counselling).

# 6 Architecture of the School Pilot

## 6.1 System Overview

The school pilot itself resides on a server, with user access through thin clients (web browsers), although users also need a local ABC client with their smart card readers. The EDOC system connects to different ABC Systems for all handling of credentials.

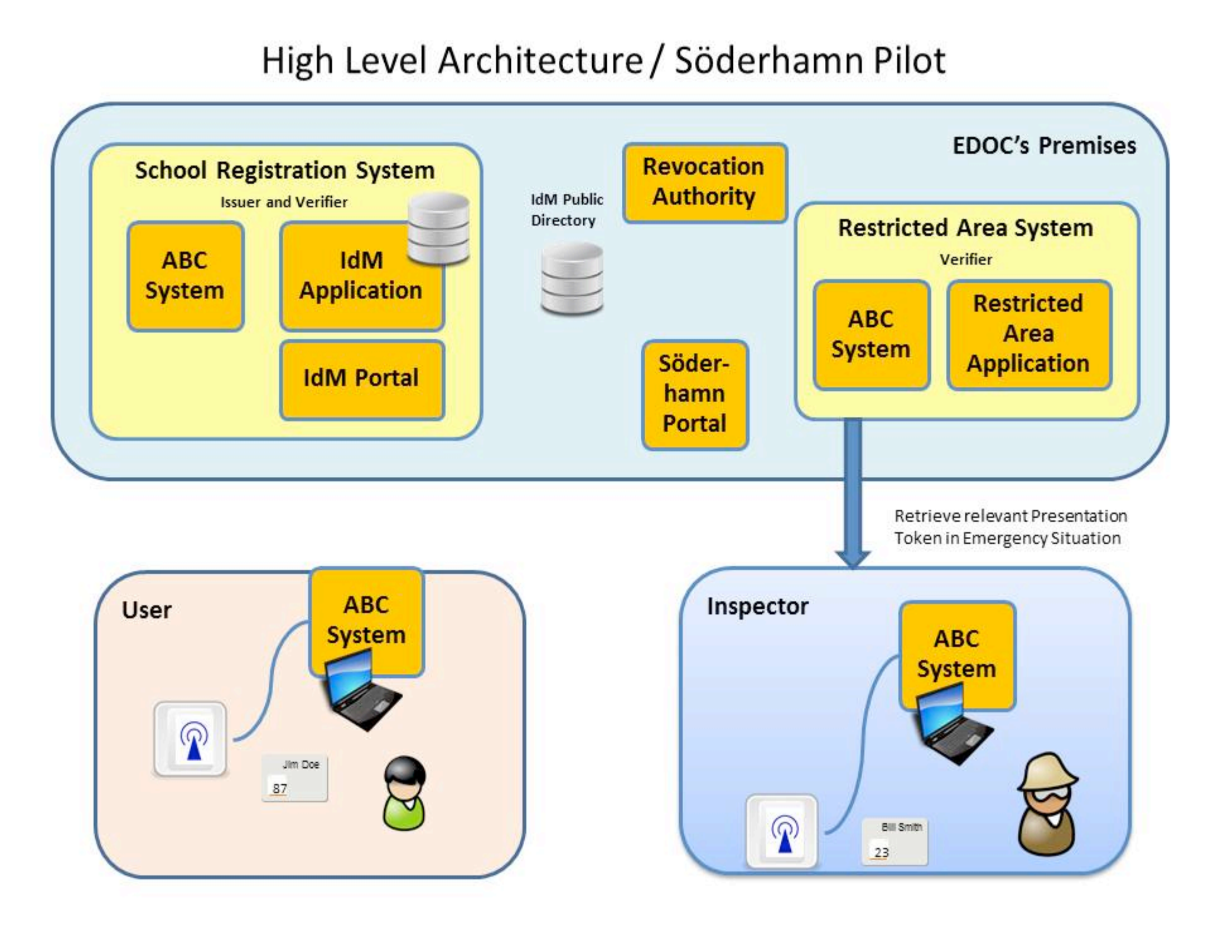


**Figure 14: High Level Architecture/Söderhamn Pilot**

As can be seen from Figure 14, the architecture of the Söderhamn pilot is based on various components. These components have different functionalities based on the scenario and use case definition of this pilot.

***School Registration System***: 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 access to those Users (i.e. pupils) that satisfy certain properties.

***Inspector***: The inspector is a trusted entity like a School inspector board (impersonated by several persons from the School Inspector board jointly acting), 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 ABC Application***: This application will run locally on the user's PC and will provide the smart card interface and enable the user, utilizing their smart card, to participate in the school portal. 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.

## 6.2 Restricted Area System Architecture

The school pilot EDOC application provides the pilot functions, most notably the different kinds of Restricted Areas and access to them. It also interfaces with the IdM Portal to check credentials.

The EDOC application is built as a traditional 3-tier architecture.

| | | |
|---|---|---|
| Tier 1 | Presentation | .Net / HTML |
| Tier 2 | Application / business logic | .Net |
| Tier 3 | Data | MS SQL Server |

While the pilot application will be installed on a single server, the application is built to be able to use a database on another server. The presentation and application tiers, on the other hand, are logically separate but built together, thus always to be deployed on the same server.

A firewall can naturally be placed in front of the application, allowing only http / https traffic. If, at a future point in time, the database is installed on a server of its own, there can also be an extra security measure of another firewall or restricted router between the application and data tiers.

The EDOC application does not have any further sub-components. All user interaction is done via a web browser, while a separate component is used to connect to the IdM part of the ABC system. Also, note that the user interacts with the ABC Engine, in addition to the interaction with the Restricted Area System.

The data flows for the application are described in more details in D5.1.

The following data is stored in the EDOC application database:

- RA data
    - type of RA (general chat, counselling etc)
    - access policy
- Chat messages (each message connected to a specific RA)
- Files uploaded (each file connected to a specific RA)

- Alias list (aliases already used, thus only available to the previous user). However, the server does not store the identity of the previous user, only lets her use an alias already stored on her smart card although it is in the list.

The restricted area system interacts with the ABC System and the ABC engine for access policy control and to retrieve attributes values from the credentials. XML files are sent on the interface, on a question-and-answer basis. Each request for verification of credentials generates a response stating either an ack/nack or an actual list of the credentials asked for.

The restricted area system has no incoming interfaces to other applications.

## 6.3 IdM Portal Architecture

The IDM Portal is the frontend the user-facing part of the university registration system. During the early phase of the trial it supports bootstrapping the ABC4Trust system, including selection of courses the students will attend. The IDM portal provides the administration interface to the users, to change their persistent-non-anonymous data.

The IdM Portal includes the ABC functionality of an issuer. This function is based on the ABC Engine functionality.

For Bootstrapping the IDM includes a SAML IDP functionality. Hereby the password is a onetime password, which is issued to the users for initial use.

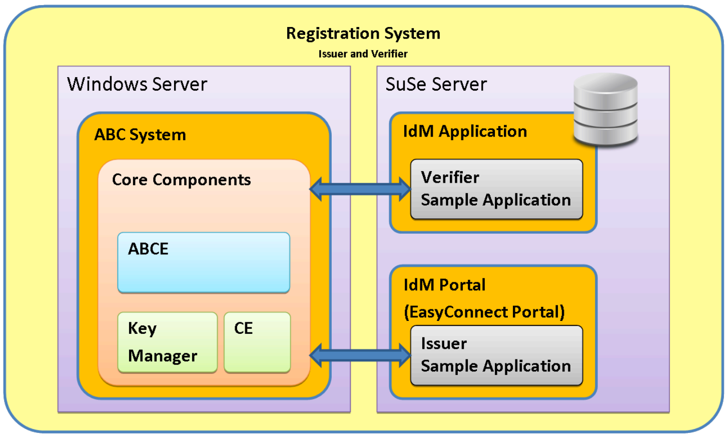


**Figure 15: IDM Portal and IDM Application Architecture**

The IDM Portal does not have further sub-components, but is one application with interfaces to the User Client (Web Browser) and IDM Application.

The Interface to the User Client is compliant to HTML & HTTP including the standard SAML based interface toward service providers (e.g. the school or university registration system). To learn about SAML please see e.g. Eve Maler's SAML tutorial[5].

As the portal does not have a database of the attributes of the user, the IDM application will be queried. The Privacy ABC credentials issued by the IDM portal are stored by the user and used to create tokens, which are transferred to the service, but no direct communication interface exists between Service Provider and IDM Application.

[5] http://www.itu.int/itudoc/itu-t/com17/tutorial/85573.html

No persistent data is stored in the IDM Portal, but data from the IDM Application or from the IDM ABC System is forwarded to the user.

## 6.4 IdM Application Architecture

For a diagram of the IDM application, please see Figure 15.

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

Two main components exist in the IDM Application, the SAML IDP and the ABC4Trust verifier. The SAML IDP works according to the SAML specification. It may provide an authentication of the user based on of several “out of bound” authentication methods. In the ABC4Trust pilots only OTP and ABC4Trust Token authentication will be used.

The IDM Application has no own web browser interface as such, users will not “visit the IDM application” without being specifically redirected by a service provider to it. Then the only interface that might be shown in a web browser is a username/One Time Password login screen.

The IDM Application will store the information, or get ABC Tokens by the user. The information will be evaluated, verified and a SAML reply given.

We differentiate between internal and external interfaces. The IDM Application – IDM Portal internal interfaces that no other component in the trial needs to interface with are just named for completeness reasons, but not further elaborated.

Details about the external interface toward the ABC System can be found in Deliverable 2.1; only the external API functions of the ABC Engine are utilized. The external interface to a SAML client is according to the standard and details can be found in [SAML].

In its function of a verifier tokens from the user client can be received and handled, but no direct interface to the issuer, or to handle ABC credentials exist.

Internal Interfaces of:

- Database Adaption Layer: Database Interface, Data Adaption Layer To IDM Portal, Data Adaption Layer to Service Provider Output, To Authentication Pipeline
- Authentication Pipeline: To Database Adaption Layer, To Service Provider Output Interface
- Service Provider Output Interface: To Database Adaption Layer
- Configuration Interface: Configuration File Reader

# 7 Project Plan

## 7.1 Time Line

**Error! Reference source not found.**Figure 16**Error! Reference source not found.** shows the development of the Söderhamn pilot in relation to the overall time line of the ABC4Trust project. **Error! Reference source not found.** In particular it shows the time line for the development iterations and pre-pilot. The content of each iteration is explained analytically in section 7.3.

## 7.2 Software Development Roles needed

The following roles are used during the pilot development and production start. Some roles may have several people, and one person can take on several roles.

Project lead

The project lead takes on traditional project management tasks, such as maintaining the timeline and managing resources.

System analyst

The analyst makes sure the use cases are properly defined and cover all of the functional requirements. This is also the role handling change requests.

System architect

The system architect handles architectural tasks, as well as the overall system design and database design. The architect is also the person responsible for the transfer of functional requirements to technical solutions.

Programmer

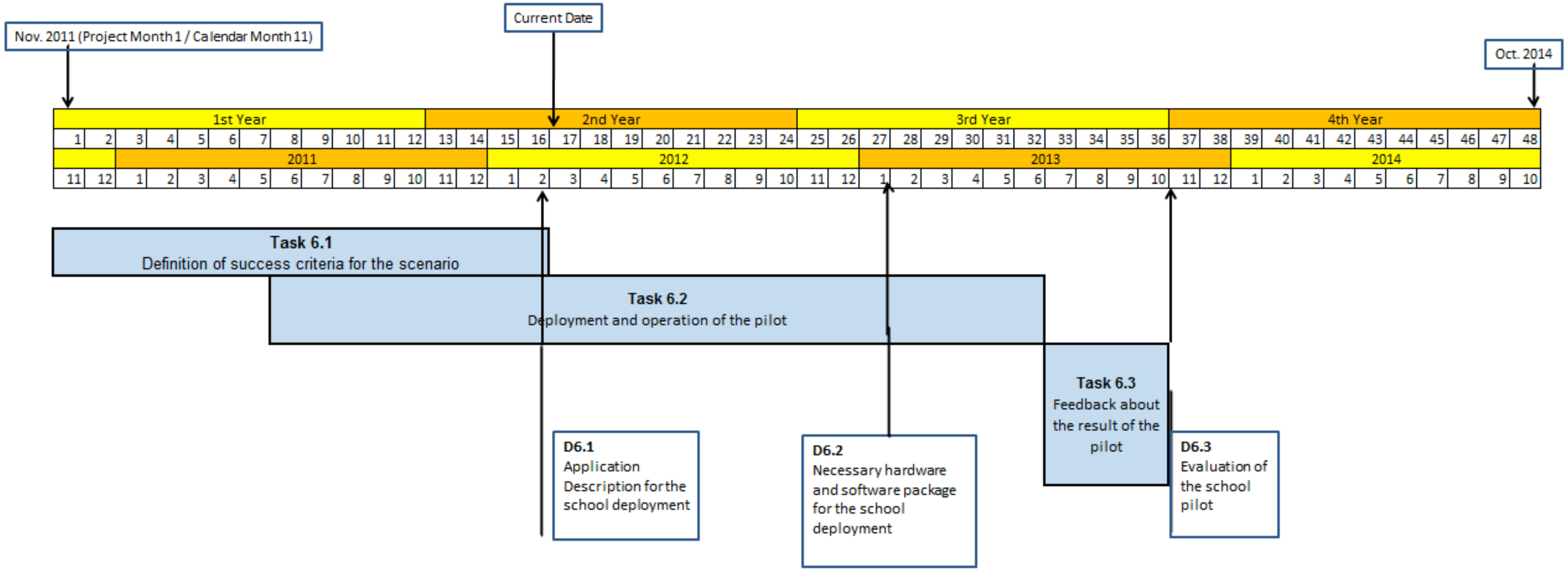
The programmer details the system and database design and creates the actual code needed to implement it, as well as documentation of code modules.

Test designer

The test designer specifies test cases from the requirements.

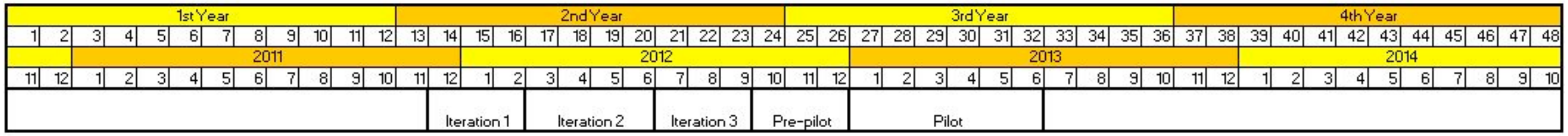
Tester

The tester performs the actual tests, documents them and makes sure the results are given as feedback to the programmer and architect. Thus, the tester should not be the same person as the programmer.


Nov. 2011 (Project Month 1 / Calendar Month 11)
Current Date
Oct. 2014
Task 6.1
Definition of success criteria for the scenario
Task 6.2
Deployment and operation of the pilot
Task 6.3
Feedback about the result of the pilot
D6.1
Application Description for the school deployment
D6.2
Necessary hardware and software package for the school deployment
D6.3
Evaluation of the school pilot

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1st Year | | | | | | | | | | | | 2nd Year | | | | | | | | | | | | 3rd Year | | | | | | | | | | | | 4th Year | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| | | 2011 | | | | | | | | | | | | 2012 | | | | | | | | | | | | 2013 | | | | | | | | | | | | 2014 | | | | | | | | | |
| 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

**Figure 16: Overall timeline**



| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1st Year | | | | | | | | | | | | 2nd Year | | | | | | | | | | | | 3rd Year | | | | | | | | | | | | 4th Year | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| | | 2011 | | | | | | | | | | | | 2012 | | | | | | | | | | | | 2013 | | | | | | | | | | | | 2014 | | | | | | | | | |
| 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | | | | | | | | | | | | | Iteration 1 | | | Iteration 2 | | | | Iteration 3 | | | Pre-pilot | | | Pilot | | | | | | | | | | | | | | | | | | | | | |

**Figure 17: Development iterations and pre-pilot timeline**

## 7.3 Iterations

The school pilot will be built using an iterative approach. Each iteration has its targets and will deliver code as well as documents. At the end of each iteration, the result will be tested, and test results will be part of the input for the next iteration.

### 7.3.1 Iteration 1

#### 7.3.1.1 Targets

The first iteration will encompass requirements as well as a first demo system for the pilot. At this point, the system will not include integration with the ABC systems, only a base for the pilot's own functions and a temporary login module where the ABC login will be integrated later.

Iteration 1 will deliver requirements (in this document), an architectural outline (also in this document), test cases for the functions developed in iteration 1, and the code base for the following functions:

- Create a Restricted Area for chat, counselling or document share.
- Access a Restricted Area, with a check for credentials (using dummy credentials).
- Chat function, to be used in chats and counselling sessions.
- Document upload and download functions.
- A temporary login and credentials module, for test purposes.

Thus, the functions above will all be available and ready for test. At the end of the iteration, tests will be performed for those functions.

#### 7.3.1.2 Roles used

The following roles will be used in iteration 1:

Project lead, system analyst, system architect, programmer, test designer, tester.

### 7.3.2 Iteration 2

#### 7.3.2.1 Targets

The second iteration will focus on integration with the ABC system, thus creating modules to integrate login as well as fetching and verifying credentials. It will also take care of bugs reported from iteration 1.

Iteration 2 will deliver the remaining test cases, architectural adjustments (if needed) and system design for the integration, and code to perform all functions needed in the interaction with the ABC system.

The code base for the following functions will be delivered by iteration 2:

- Log in to the system.
- Access a Restricted Area, with a check for (real) credentials.
- Add and revoke credentials.
- Alias database.
- Dashboard functions.

Thus, the functions above will all be available and ready for test. At the end of the iteration, tests will be performed for those functions.

#### 7.3.2.2 Roles used

The following roles will be used in iteration 2:

Project lead, system architect, programmer, test designer, tester.

### 7.3.3 Iteration 3

#### 7.3.3.1 Targets

The last iteration will, of course, include remaining functions. The last iteration will contain the functions needed for inspection as well as functions to remove previously entered data from view, as well as functions to delete it entirely.

The code base for the following functions will be delivered by iteration 3:

- Inspector login.
- Inspector reading chat content, including text removed from view.
- Inspector request to see presentation tokens.

Thus, the functions above will all be available and ready for test. At the end of the iteration, tests will be performed for all the pilot's functions, and a bug fix period will be planned at the end of the iteration.

#### 7.3.3.2 Roles used

The following roles will be used in iteration 3:

Project lead, programmer, and tester.

### 7.3.4 Pre-pilot

After the development iterations, a pre-pilot will be run. This is an extensive test, using smart cards issued for real users. During the pre-pilot, there will be continual bug fixes and adjustments to make the system run smoothly.

# 8 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.

Civic Registration Number (personnummer in Swedish)

Every person living in Sweden has a 10 digits long unique personal identification number called “Personnummer”. This Personal Identity Number contains or consists of two parts: the birthdate of the person and a 4 digits serial number, YYMMDD-XXXX (640512-3875). It is mandatory to have this number and it is widely used by all public authorities, banks, insurance companies and other such as employers and schools. Today the school already has access to and is using the personal number of all pupils and their parents and all school personnel.

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 Inspection Board

The Data inspection board (Datainspektionen) is a Swedish government organization overseeing rules on all databases in digital form containing personal data as well as all Internet publication of personal data.

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 artefact 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.

Restricted Area

> The internal representation of a chat, counselling session or document area. Every restricted area has a set of restrictions (attributes) to be matched to credentials. Only users with matching credentials can access the restricted area.

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

# 9 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

Personal Unblocking 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

# 10 Bibliography

[Art29WP160] Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)*, Adopted on Adopted on 11 February 2009, 2009, online:

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

[HSWH2011] Hans Hedbom, Jan Schallaböck, Rigo Wenning, Marit Hansen. Contributions to Standardisation. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) *Privacy and Identity Management for Life*, pp. 479–492. Springer, Berlin (2011)

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

[KLNPZ11] Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Harald Zwingelberg. ABC4Trsut Deliverable D2.1 “Architecture for Attribute-based Credential Technologies – Version 1”, online: https://abc4trust.eu/index.php/pub/107-d21architecturev1

[PfiHan2010] Andreas Pfitzmann, Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, (2010), online: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[SAML] Security Assertion Markup Language 2.0, OASIS

[ZwiHan2012] Harald Zwingelberg, Marit Hansen. Privacy Protection Goals and Their Implications for eID System. In Simone Fischer-Hübner, et al., editors, *Proceedings of the IFIP Summer School 2011*, Springer Boston, to appear 2012.