

D6.3 Evaluation of the School Pilot

Souheil Bcheri, Erik Björk, Daniel Deibler, Göran Hånell, Jimm Lerch, Maksym Moneta, Monika Orski, Eva Schlehahn, Welderufael Tesfay

<i>Editors:</i>	<i>Souheil Bcheri (EDOC), Jimm Lerch (EDOC)</i>
<i>Reviewers:</i>	<i>Joerg Abendroth (NSN), Welderufael Tesfay (GUF)</i>
<i>Identifier:</i>	<i>D6.3</i>
<i>Type:</i>	<i>Deliverable</i>
<i>Version:</i>	<i>1.0</i>
<i>Date:</i>	<i>2/05/2014</i>
<i>Status:</i>	<i>Final</i>
<i>Class:</i>	<i>Public</i>

Abstract

This document describes the conclusions from the first and second round of the ABC4Trust Söderhamn school pilot, including user evaluation and a brief evaluation of each component of the pilot while including conclusions on legal topics as well as recommendations for different stakeholders.

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	Belgium
7.	Miracle A/S	MCL	Denmark
8.	Nokia Solutions and 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.

Copyright 2014 by EDOC, GUF, SK, ULD.

List of Contributors

Chapter	Author(s)
Executive Summary	Souheil Bcheri (EDOC), Jimm Lerch (EDOC)
Chapter 1	Souheil Bcheri (EDOC), Maksym Moneta (EDOC), Monika Orski (EDOC)
Chapter 2	Souheil Bcheri (EDOC), Maksym Moneta (EDOC), Monika Orski (EDOC)
Chapter 3	Souheil Bcheri (EDOC), Maksym Moneta (EDOC), Monika Orski (EDOC)
Chapter 4	Eva Schlehahn (ULD), Daniel Deibler (ULD), Welderufael Tesfay (GUF)
Chapter 5	Eva Schlehahn (ULD), Daniel Deibler (ULD)
Chapter 6	Souheil Bcheri (EDOC), Erik Björk (SK), Göran Hånell (SK)
Appendix A	Souheil Bcheri (EDOC)
Appendix B	Souheil Bcheri (EDOC)
Appendix C	Souheil Bcheri (EDOC)
Chapter 7	Bibliography

Executive Summary

This document focuses on the description and analysis of the user evaluation results from the first and second rounds of the Söderhamn school pilot conducted within the scope of WP6 of the ABC4Trust project. The goal of the pilot was to employ Privacy-ABC technologies into a school interaction system that allowed pupils, school personnel and parents to interact in chat rooms and information areas. The interactions were anonymous when they choose for it to be so, while their personal attributes (credentials) remain verifiable throughout the process. The design, implementation and testing of the pilot system was based on the use cases, pilot requirements and pilot system architecture documented in deliverables [D51], [D61], and [D62] respectively while the technical aspects of the deployment are elaborated in [D53].

This document begins with a brief examination of the timeline and content of the two rounds of the school pilot as well a review of the relevant legal and survey-related documentation. The pilot scenarios are subsequently presented in more detail in order to demonstrate their connection with the evaluation process. Success criteria of the pilot is appraised in context with the degree to which the realization of the two rounds met these criteria. Next, the findings of the evaluation of the pilot are described. User reactions and intersection with the pilot system are shared and an evaluation of the pilot's components is consequently made, centered on the impact on user experience. An evaluation of the legal aspects and impact of using Privacy-ABC follows. Finally, this report provides a comprehensive list of recommendations for further development in using Privacy-ABC.

To sum up, the two rounds of the school pilot were successful. The goal, which was to deploy the new cryptographic architecture to showcase the Privacy-ABCs technology features, as well as the Restricted Areas application, was achieved.

Table of Contents

1	Introduction	10
1.1	Purpose of this Document.....	10
1.2	Structure of the Document.....	10
1.3	The aim of the School Pilot.....	11
1.4	A Brief Introduction of the Two Pilot Rounds	12
2	School Pilot's Scenarios	13
2.1	Pilot Overview	14
2.2	Pilot Users and Roles	16
2.3	An Introduction to the Restricted Area Application.....	16
2.4	Functionalities and Execution of First Round.....	18
2.5	Functionalities and Execution of Second Round	19
3	Evaluation of School Pilot's Deployment	25
3.1	Requirements and Fulfillments	25
3.2	Specific Considerations for the Second Round	27
3.3	Statistics	27
3.4	Evaluation of School Pilot's Network.....	28
3.5	Evaluation of School Pilot's Services/Applications	29
3.6	Evaluation of Smart Cards and Readers	29
3.7	Evaluation of School Pilot's System Security.....	31
3.8	Evaluation of School Pilot's Availability	31
3.9	Evaluation of School Pilot's Response Time	31
3.10	Evaluation of the Restricted Area System	32
4	User Evaluation Results	34
4.1	First round questionnaire summary.....	34
4.2	Evaluation of User Experience and Feedback.....	35
4.2.1	Functionalities of the system and their utilisation	35
4.2.2	Usability and Transparency	39
4.2.3	Comprehension of the ABC system	40
4.2.4	Trust and Acceptance.....	43
4.3	Evaluation of User Experience and Feedback: User Acceptance of Privacy-ABC	46
4.3.1	Perceived usefulness for privacy protection.....	46
4.3.2	Perceived ease of use	47
4.3.3	Perceived anonymity	47
4.3.4	Privacy-ABCs trustworthiness	48
4.3.5	Subjective Norm	48
4.3.6	Behavioural intention to use	48
5	Considerations on Legal Topics	50
5.1	Applicable Law	50
5.2	Consent Form and Informing of Users	50
5.3	Inspection.....	52
5.4	Data Subjects' Rights	54
5.5	Deletion of Personal Data.....	56

6	Recommendations and Conclusion	57
6.1	General recommendations	57
6.2	Recommendations for improved performance.....	57
6.3	Recommendations for Inspection	58
6.4	Recommendations for developers	58
6.5	Recommendations for the Restricted Area Application.....	58
6.6	Recommendations from the school administration	59
6.7	Conclusion	60
Appendix A	User's Questionnaires	61
A.1	User's Questionnaire - First round - English version	62
A.2	User's Questionnaire - First round - Swedish version	63
A.3	User's questionnaire - Second round - English version.....	65
Appendix B	Legal Forms	72
B.1	Information sheet for pupils/participants and parents/legal guardians - English version	73
B.2	Consent form for pupils/participants and parents/legal guardians - English version	79
B.3	Information sheet for school staff - English version	82
B.4	Consent form for school staff - English version.....	88
B.5	Legal Notice and privacy policy of the website - English version.....	90
Appendix C	User Manual.....	92
C.1	User Manual - Söderhamn round 1 - English version	93
7	Bibliography.....	170

Index of Figures

Figure 1: Informational meeting for students	11
Figure 2: Second round preparation – Introduction and distribution of smart cards to guardians. 12	
Figure 3: School Portal - Start page	13
Figure 4: Overview of the school pilot	14
Figure 5: The Restricted Area Application - A List of Restricted Areas	17
Figure 6: RA Look & Feel	19
Figure 7: Smart card design	20
Figure 8: New Restricted Area Application layout.....	21
Figure 9: Chat in RA.....	22
Figure 10: Reported message in chat	23
Figure 11: School Inspection Board view.....	24
Figure 12: Swedish pilot on the Swedish national TV.....	25
Figure 13: Smart card and card reader	30
Figure 14: Opinion from the first round questionnaire	34
Figure 15: Participant Distribution	35
Figure 16: Results of question 1	36
Figure 17: Results of question 6	37
Figure 18: Results of question 9	37
Figure 19: Results of question 11	38
Figure 20: Results of question 4	38
Figure 21: Results of question 2	39
Figure 22: Screenshot to question 2.....	39
Figure 23: Results of question 7	40
Figure 24: Screenshot to question 3.....	41
Figure 25: Results of question 3	41
Figure 26: Screenshot to question 5.....	42
Figure 27: Results of question 5	43
Figure 28: Results of question 8	44
Figure 29: Results of question 10	44
Figure 30: Results of questions 12 and 13	45
Figure 31: Results of question 14	46
Figure 32: List of inspectable RA indicated with the 'eye sign'.....	53
Figure 33: Inspection indicator - Alias "Superman1000" has been used in an inspectable RA.....	54
Figure 34: Inspection indicator - Alias "Anonymous" has not been used in an inspectable RA ...	54
Figure 35: Identity Selector with Inspection warning reminder	54
Figure 36: Access Policy Editor GUI - a more User friendly Version	59

Index of Tables

Table 1: Restricted Areas created in second round	27
Table 2: Aliases used in second round	28
Table 3: Content in Restricted Areas.....	28
Table 4: Measurement of timing (all times are in seconds)	32
Table 5: Performance Measurements	32

1 Introduction

The ABC4Trust project conducted pilots of Privacy-ABC deployments in two separate production environments in order to provide real user feedback on Privacy-ABC systems. The ABC4Trust gathered practical experiences with Privacy-ABC applications in two related, but differing scenarios within two pilots: 1). a student course evaluation system in Patras¹, and 2). the Söderhamn school communication and interaction system. The testing conducted within these two environments allowed for the opportunity to test the credentials usage and performance with two user groups of differing skills and needs. One of the groups were users at a school in Söderhamn, Sweden. This pilot provided feedback of distinct value to the developers of the reference implementation as well as to other key project players.

1.1 Purpose of this Document

The Swedish pilot in Söderhamn consisted of several types of user communication interactions utilising Privacy-ABC for unique credential verification that were needed by the school. This document builds upon the deployment and implementation of these services as well as evaluates the overall efficacy of these operations. Additionally, this document intends to share some of the knowledge gleaned from the experience and provides some lessons learned from the Söderhamn school pilot. In addition to outlining some very specific technical situations and challenges that were encountered over the course of the pilot, this document also incorporates non-technical experiences and feedback from the questionnaires resulting from the two pilot rounds as well as includes an extensive examination of the legal aspects surrounding the pilot.

The final purpose of this document is to demonstrate the overall fulfilment of the original pilot objectives as further elaborated in [D61].

1.2 Structure of the Document

Chapter 1 introduces the school pilot and this document.

Chapter 2 provides an introduction to the scenarios implemented in the first and second rounds of the school pilot.

Chapter 3 provides a high-level description of the criteria and requirements that were used in order to evaluate the success of the pilot development and operation. Moreover, it presents a description of the evaluation of the pilot's components and their respective services and applications.

Chapter 4 provides evaluation data collected from the pilot's users, as well as descriptions of how the data was collected. It also includes a description of the understanding and acceptance of the Privacy-ABCs technology by the participating users.

Chapter 5 provides an evaluation and discussion of the legal aspects of using Privacy-ABC, within the specific context of the Söderhamn school pilot.

Chapter 6 contains recommendations for further development and use of Privacy-ABC as derived from the Söderhamn school pilot.

¹ Additional information regarding the student course evaluation system in the Patras pilot can be found in [D71] and [D73].

Appendix A contains the questionnaires used for user the evaluation, with further explanation of the procedure that provided the results described in chapter 4.

Appendix B contains the legal forms that were presented to the users in the two rounds of the pilot.

Appendix C contains the English version of the Söderhamn round 1 user manual that was available to the users during the pilot.

Chapter 7 contains the bibliography.

1.3 The aim of the School Pilot

The aims of ABC4Trust pilots were threefold: to deepen the understanding in Privacy-ABC technologies; enable their efficient/effective deployment in practice; and test their federation in different domains. To this end, the outputs ABC4Trust project are:

1. Produce an architectural framework for Privacy-ABC technologies that allows different technological realizations to coexist, be interchanged, and federated as it:
 - a. Identifies and describes the different functional components of Privacy-ABC technologies, e.g. request and issuance of credentials and for claims proof; and
 - b. Produces a specification of data formats, interfaces, and protocols for this framework.
2. Define criteria to compare the properties of realizations of these components in different technologies; and
3. Provide reference implementations of each of these components.

Within this context, the Söderhamn School pilot implemented a range of chat and information exchange functions, called Restricted Areas (RAs), to be used by school personnel, pupils, and the pupil's parents or legal guardians. These functions included, but were not limited to: chat rooms for pupils and/or staff; online counselling sessions where staff can provide counselling in a safe environment where 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.



Figure 1: Informational meeting for students

1.4 A Brief Introduction of the Two Pilot Rounds

The school pilot took place in Norrtullskolan, a combined elementary and secondary/comprehensive school, located in Söderhamn, Sweden. It was included as an ABC4Trust project in order to demonstrate the realisation that applications using Privacy-ABCs preserves the anonymity of the users while offering the required level of privacy. The school pilot used Privacy-ABC technologies to enable secure authentication in communications between pupils, guardians, parents and school personnel. The ABC4Trust architecture took into account the issues of identity, anonymity and privacy, and combined them into a single solution.

The pilot in Söderhamn considered several types of communication needed by the school:

- Chat communication
- Political discussions
- Counselling with health personnel
- Documents access and sharing

The pilot functions were provided in two distinct phases. The 1st round of the Söderhamn pilot, which involved 10 teachers and 22 pupils, started on May 13, 2013 and ended on June 10, 2013.

The duration of the 1st round of the Söderhamn pilot was extremely short. Originally, this round of the pilot was planned to be launched end of Jan. 2013, but delays and obstacles in the smart card area coupled with the fact that this pilot was the first to make use of many new ABC4Trust features (specifically revocation and reissuance), meant that the start of the 1st round had to be delayed for more than 3 months. While the original plan was to run only one round of the pilot, the aforementioned delays unfolded in such a way as to make it necessary to execute a first round of the pilot to test the basic functionalities and to give end-users the opportunity to provide vital feedback for the final execution of the main pilot (the second round).

Based on the experiences and feedback garnered from the 1st round, the 2nd round of the pilot commenced on October 14, 2013 and concluded on Feb. 28, 2014 with the involvement of the 381 participants that had signed the consent form.



Figure 2: Second round preparation – Introduction and distribution of smart cards to guardians

2 School Pilot's Scenarios

The different pilot scenarios involved pseudonymous community access and social networking, as well as anonymous student counselling and medical advice. The community used Privacy-ABC technologies to protect the users' (pupils, guardians and school personnel) identity against theft while protecting their anonymity and privacy. On one hand, pupils were able to identify themselves to access restricted chat rooms and restricted information. On the other hand, they were allowed to remain anonymous to school personnel when asking private and sensitive questions, while being assured that school personnel communicated only with authorized pupils of the respective school or class.

The School Portal (www.abc4trust.se) was the starting point of the school pilot application. This was a website that contained not only general information about the pilot, but also provided links to the required software and applications to be employed by the pilot's users in addition to other support materials. The School Portal (see Figure 3) user interface incorporated the same design concept as the Restricted Area Application (see Figure 5).

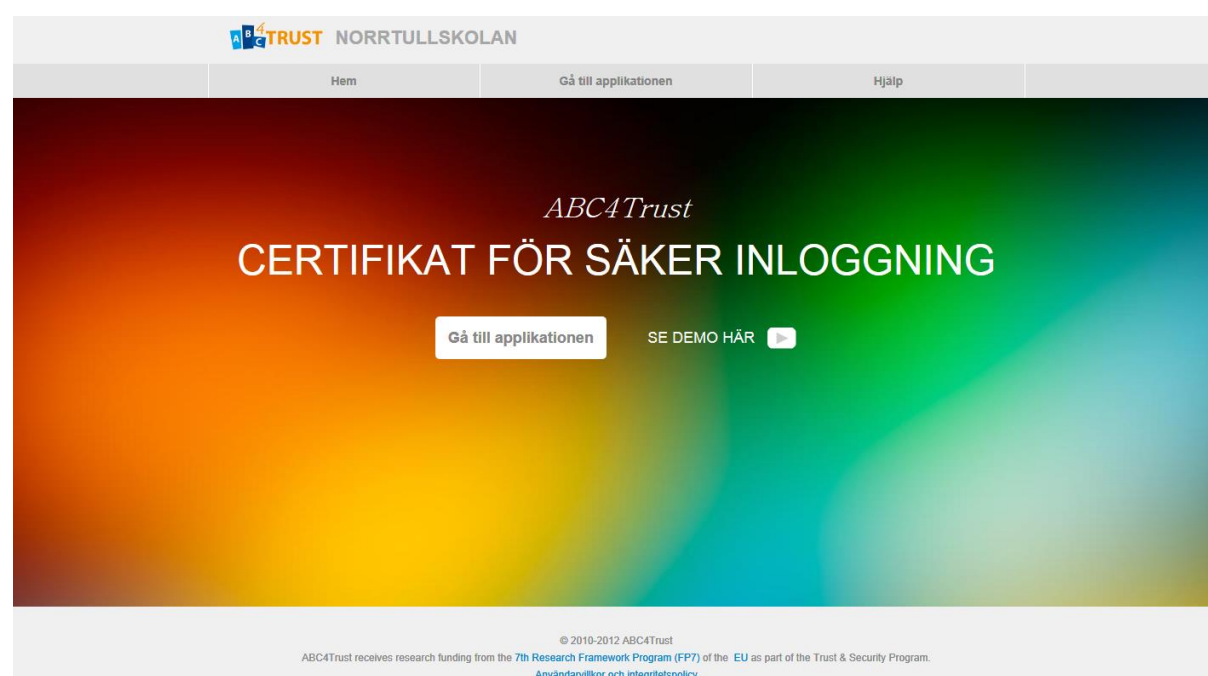


Figure 3: School Portal - Start page

Figure 3 is a screenshot of the School Portal home page which consisted of a menu (links) to the following different web pages. (Swedish translation within the parenthesis):

- Home (Hem): Link to the home page.
- Enter the application (Gå till applikationen): Link to the Restricted Area Application which required logging in using Privacy-ABC technologies (smart cards with Privacy-ABC credentials).
- Help (Hjälp): Contained the FAQ, User Manual and links to download the following: User Application Installer, IdM Portal and the smart card reader drivers.
- See demo here (Se demo här): A link to instructional video available at the ABC4TrustSverige YouTube channel: <http://www.youtube.com/user/Abc4trustSverige>.

2.1 Pilot Overview

The pilot site was at Norrtullskolan, a combined elementary and secondary/comprehensive school, located in Söderhamn, Sweden. Söderhamn is a few hours drive north from Stockholm, with a population of nearly 26,000 inhabitants. The school is educating approximately 580 pupils from the age of six to sixteen and has about 80 employees. The target group of the pilot were the teachers and pupils from the 7th through the 9th grade along with the students' guardians. Out of this target group, the pilot consisted of 381 participants able to engage in the pilot, all of whom had voluntarily given their permission by signing the consent form.

Over the years the school personnel have sought to make this school the best environment for both students and teachers. Norrtullskolan has a vision to eradicate all bullying, discrimination and other self-esteem lowering treatments, and encourage the pupils actively involved in this process.

Additionally, Norrtullskolan has vigorously adopted computers and technology into the pedagogical process within their educational system. Computers are used not only by the school personnel, but also by the pupils as a fundamental part of the curriculum. Thus, the school network and computer literacy were already well-grounded and established.

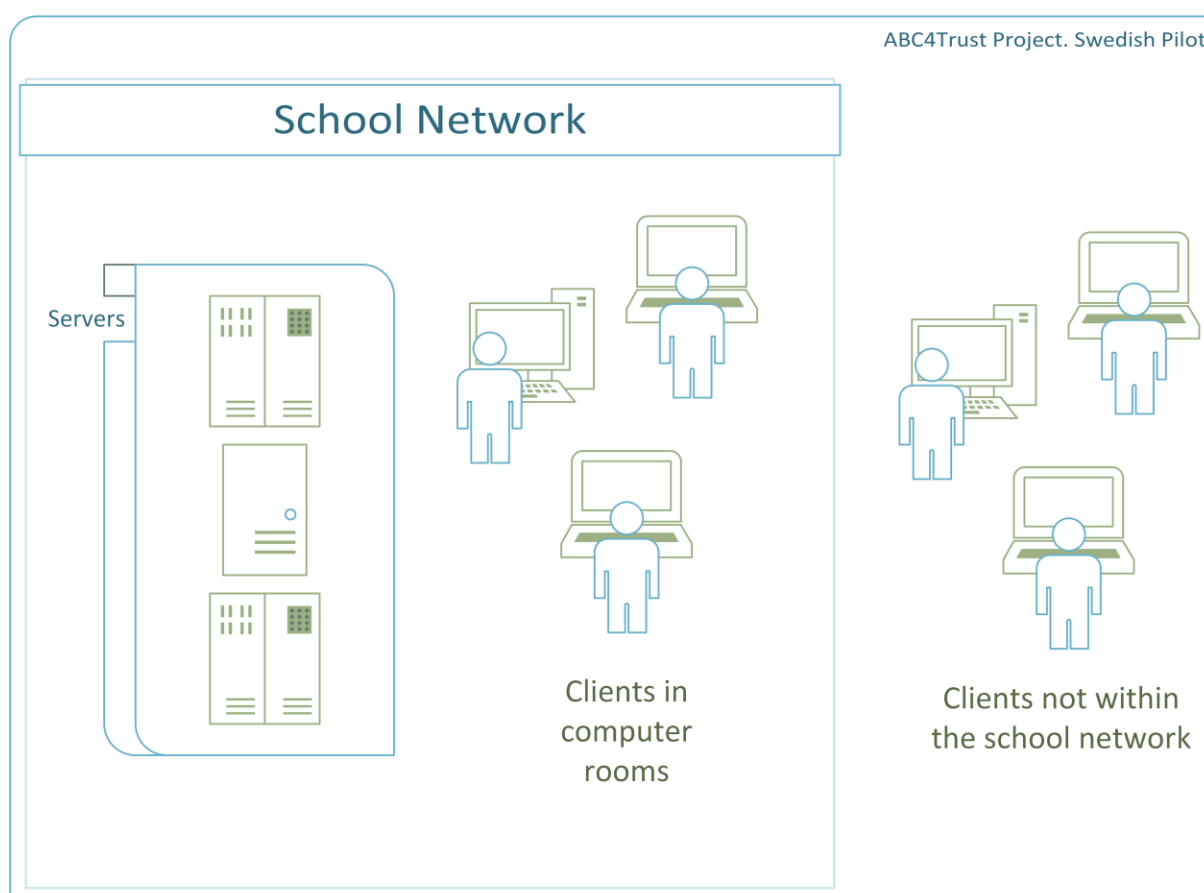


Figure 4: Overview of the school pilot

The school pilot context consisted of servers hosting the Restricted Area, the school registration system and the user clients. The servers were placed at Norrtullskolan in its secured server room and became an integrated part of the school's network. Clients were installed at all computers with a smart card reader attached, which included computers within the school as well as in the pupils' homes. Therefore, the Söderhamn pilot included servers within a secured network and

internal to the school, with Internet access to the servers as clients available where in users in remote locations could access the servers via the Internet.

Every user (pupil, guardian, teacher or other school personnel) participating in the Söderhamn pilot needed to have all the following:

- Smart card with corresponding PIN/PUK codes and with Privacy-ABC credentials
- Smart card reader, installed on and connected to the PC
- Windows based PC (Connected to the Internet)
- Web browser (Firefox or Internet Explorer)
- User Application (Installed on the PC)

The smart card was prepared (initialized and personalized) by EDOC when the, PIN/PUK codes and smart card reader were handed over to the user. In the first round of the pilot the user had to download her own credentials to the card. In the second round, however, the credentials were downloaded to the smart card by EDOC prior to be distributed to the user(s) (see Section 2.5). In the Söderhamn pilot, users were provided with either a U-Prove or an Idemix smart card. Each card stored credentials of only one crypto-engine type. The key length of both Idemix and U-Prove are set to 2048. This pilot was the only pilot within this project that made use of reIssuance since U-Prove smart cards needed to fetch fresh batches of tokens from the Issuer in order to enforce un-linkability (for more technical details see [D53]). From the user's perspective the two technologies were indistinguishable, in-line with the aim of the project.

The smart card reader was easy to install on a Windows-based PC as Windows automatically recognized the reader once it was plugged in and it installed the smart card drivers. Each user in the pilot receives a smart card reader from EDOC.

The school already had a number of public, Windows-based PC laptops that they allowed the pupils to use. While the pupils have to share those laptops with other pupils, the teachers have their own laptops that are different from the laptops used by the pupils. The laptops used by teachers and those used by pupils have different configurations and have access to divergent networks. The school has two networks for different users. The first network, called "Skolnet4you.soderhamn.se", is publicly open and requires no passwords. This network is used primarily by pupils and visitors, but teachers can also use it because it's public. The second network, called "admin.soderhamn.se", is password protected because it's accessible only to teachers, counselors, nurses, administrators and the schoolmaster. As the teachers' computers required administrator permission to install programs, EDOC had to ask the school administrators for permission to do the installation of all necessary components for the ABC4Trust pilot.

In most instances Internet Explorer and/or Firefox web browsers were already pre-installed on the school computers, but EDOC installed them if they were not present. EDOC handled the installation of the User Application on all the school computers. Users that wanted to access the system from home needed to install the User Application on their home computers.

In order to be able to make use of the Privacy-ABC technologies and participate in the pilot the user had to install the User Application. This was achieved by simply clicking on the Installer link found under the "Help" section at the School Portal (<https://ra.abc4trust.se/Help>). The browser plugins were also installed automatically by the same Installer. These details were further elaborated within User Manual in the "Help" section in a step-by-step manner.

Further details of the technical structure and deployment of the school pilot have been documented in [D62].

2.2 Pilot Users and Roles

The school pilot scenarios involve users with the following roles:

- Pupils
- Guardians
- School personnel
 - Teachers
 - Counselors
 - Administrators
- School Inspection Board
- Inspectors

Any user that could access a Restricted Area (RA) was able to use such functionalities as chat, post on a wall and upload/view documents. School personnel could have special roles like School Inspection Board, Inspector or Counselor, and have the capability to represent multiple roles or not possess any such special roles and be labeled as a teacher. The main difference between school personnel and pupils/guardians was that while both categories were able to create new Restricted Areas, when school personnel created a Restricted Area using their default alias, the RA was marked as official; meaning that it was created by an official representative of the school. Additionally, the Counselors role provided the possibility for the personnel to receive requests from users for a chat within the Restricted Area designated specifically for counseling.

School Inspection Board consisted of school personnel and representatives for pupils and guardians. The School Inspection Board undertook all decisions concerning reported content – ignore, delete or send it to inspection. The Inspectors' role included the possibility to use the Inspector Application in order to make an inspection based on a request from the School Board. For the purpose of this pilot, the inspector was the schoolmaster.

Different roles and corresponding scenarios were successfully implemented and tested during the two rounds of the pilot within the functionalities used for each of them.

2.3 An Introduction to the Restricted Area Application

The Söderhamn school pilot made use of Privacy-ABC technologies integrated into the Restricted Area Application in order to, via minimal data disclosure, enable secure identification in communications amongst staff, pupils and guardians. The pilot application at Norrtullskolan involved privacy-preserving community access and internal, school-related social networking for pupils via this specifically dedicated online platform. This pilot addressed the specific challenges posed by the fact that Internet users have become younger and in many cases are minors (Pupils 12-16 years old).

The communication services provided on the online platform encompassed the following possibilities for the users to participate in:

- Chat rooms to be used by pupils and/or staff and guardians
- Online forums allowing for the discussion of lessons or other school related matters as well as for political discussions. These could be set up as openly accessible forums or as personal Restricted Areas where only a predefined group of participants can enter (e. g. children of a certain age or class).
- Online counseling sessions in restricted areas with health personnel (counsellors, social workers, nurses, coaches, etc.), where staff can provide counseling in a safe environment while pupils are not necessarily required to reveal their identity.
- Document areas where staff can share documents (e.g. grades and development plans) with pupils and their guardians.

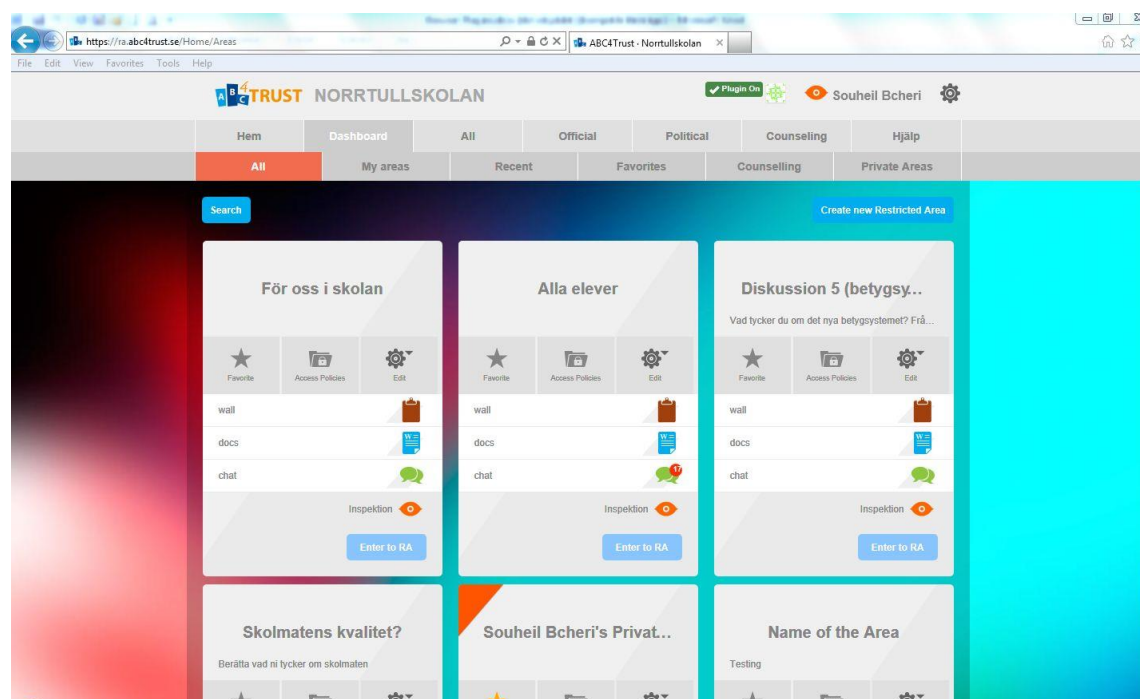


Figure 5: The Restricted Area Application - A List of Restricted Areas

As depicted in Figure 5, the Restricted Area Application consisted of many different Restricted Areas (RAs). While RAs created by the school are marked as official, other users (pupils and guardians) were also able to create new RAs for different purposes. Each RA was protected by one or several access policies² that defined the parameters regarding who was allowed to enter a specific RA, use its functionality (chat, wall, document sharing and political discussions) and access its content. For example, a Restricted Area for girls would have had the access policy “Girls”. The manner in which XML policies were generated was crucial to providing the appropriate credentials so that the users could place trust in the fact that the restrictions were in actuality true.

Users (pupils, guardians/parents and school personnel) were able to sign in to different RAs in a very secure and privacy friendly way by taking advantage of the tools provided by Privacy-ABC technologies. For example, by using her smart card a user can prove that she is a girl to enter a chat room restricted for “Girls”. This user may further prove that she belongs to Class 9A in order to enter a chat room restricted for “Class 9A”. Additionally, said user has the ability to prove that she is a girl between 14-15 years old to enter a more restrictive chat room for “Girls 14-15 years old”. In some cases, when anonymity was desired, the user could anonymously/pseudonymously sign in and participate in political discussion groups without revealing any personal data. Another case when anonymous/pseudonymous login proved to be desirable was during counseling sessions.

The access to the RA Application itself and to the different Restricted Areas was controlled with presentation policy alternatives (an XML translation of the access policies), which were verified against the credentials which the user had located on her smart card.

Some of the functionalities provided by the RA Application were the dashboard, search and browse functions for lists of Restricted Areas. Once inside a Restricted Area, users could chat,

² With ‘access policies’, the XML style ‘presentation policy alternatives’ were NOT meant. The access policies were intermediate policies which needed to be translated into PPAs via the ‘XML Generator’ before being sent to the user.

upload files and leave messages on a wall. Additional functionalities on top of the Restricted Area concept were the counseling, the political discussions, the Alias Selector, the Dashboard and the alias to alias chat (private one-to-one chat) function. Below is a description of the Alias Selector and the Dashboard that are run on the client side.

The Alias Selector handled the list of aliases owned by the user. It was designed to create new aliases, delete old ones and switch between them. Alias information was stored on the user's smart card. When the Alias Selector had to be rendered, the client made a call to the ABCE user service, via a plugin, in order to obtain the contents located within the BLOB area of the card. After the successful retrieval of the list of alias IDs and names, the corresponding aliases were rendered into UI element. Whenever an alias operation was performed, e.g. a switch between aliases, the client sent a request to the ABCE to generate a Presentation Token to compare with the one already saved in the Restricted Area database during creation. In this way, the user's aliases were saved and retrieved from the user's own smart card.

The Dashboard was the part of the client that allowed a user to see the Restricted Areas she had recently accessed, both public and private, or marked as a favourite. To avoid linkability this had to be done in separate request to the database for each alias. A list of aliases was culled from the Alias Selector so as to avoid extra requests to the smart card. The Dashboard loaded the alias IDs and made calls to the RA server to retrieve the list of Restricted Areas for the active alias.³ Then, the Restricted Areas were rendered on the Dashboard as UI elements. Thus, the Dashboard was not performing operations on the card content itself, it was there to allow for the dynamic creation of outputs that allowed the user to have a personalised start page view.

2.4 Functionalities and Execution of First Round

The following functionality was presented and used during the first round of the Söderhamn school pilot:

- Preparation and initialization of the smart cards, which included the following:
 - Initialization of hardware smart cards for Idemix and U-prove
 - Obtaining a pseudonym for the smart card
- Issuing, downloading and saving credentials to the card
- Revocation functionality
- Restricted Area application including the following functionality (see Section 2.3):
 - Documents
 - Chat
 - Wall
 - Alias Selector
 - Dashboard
 - Integration with ABCE via User Client
 - Verification of credentials for login to Restricted Areas
 - Counselling

The functionalities listed above allowed users to perform all the user scenarios planned for the first round. Basic scenarios such as logging in, accessing and using Restricted Areas, as well as communication within Restricted Areas were executed within the first round. Additional feedback details are presented further within this document.

³ Since the dashboard knew all the aliases the user had, it was specifically designed to run locally in order to prevent the possible leakage of private information.

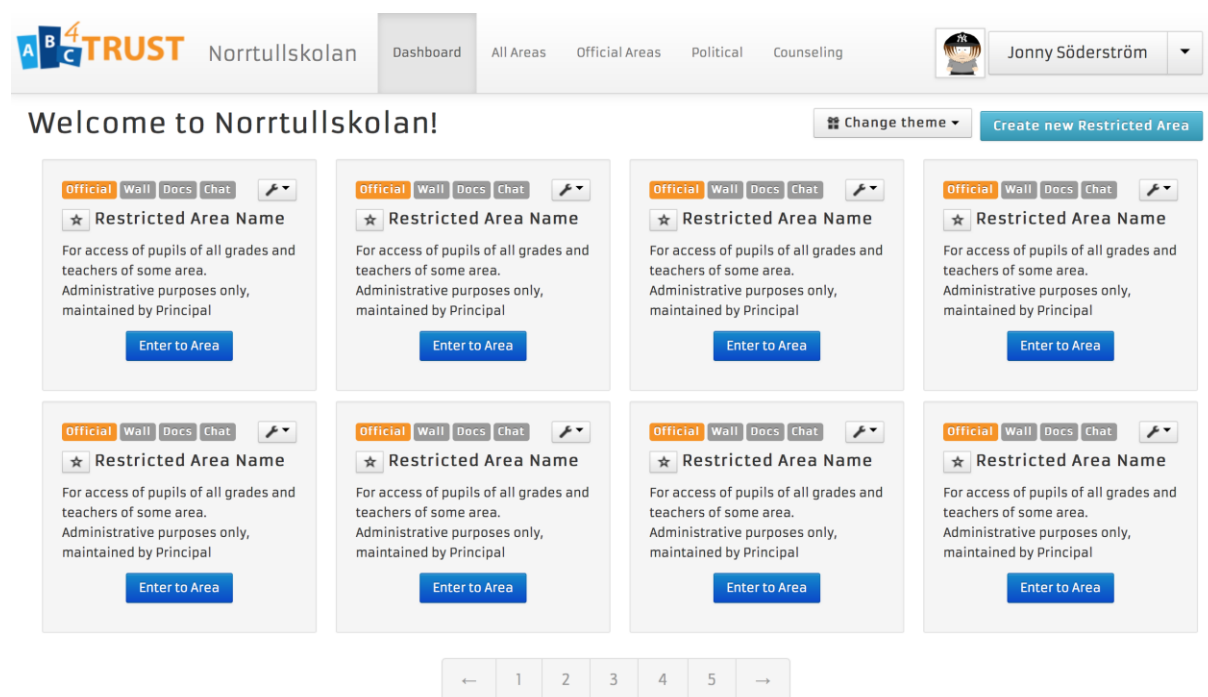


Figure 6: RA Look & Feel

Figure 6 represents one of the stages of improvement of the Restricted Area Application. Prior to the launch of the first round of the pilot the appropriate look and feel of the user interface was researched, created and further improved in order to provide a more friendly and attractive look for the younger users. Since the pilot not only considered the stability of the technical implementation of the technology, but also an example of real life usage of the system and technology, the user interface was considered crucial to the success of the pilot. Thus, the evaluation of the first round was mostly based upon the overall user experience.

Based on the results and feedback from the first round improvements were made for the second round, including changes in parts of the implementation.

2.5 Functionalities and Execution of Second Round

Due to legal issues and requirements from the school a consent form was needed to be signed prior to any level of participation in the pilot. The total number of participants who signed the consent form was 381 out of approximately 889 possible users. The distribution of users was as follows:

123 Pupils, 203 Guardians, 53 Teachers and 2 Admins.

The Second Trial included the full functionality from the first round (see Section 2.4), with improvements and bug fixes. It also included the following functions:

- Optimized performance of User Client and smart card operations
- Pre-downloaded credentials to smart cards using a new enhanced IdM Mass Provisioning Tool which replaced the functionality of the IdM Smart Card Registrar
- New layout and improved user experience of the Restricted Area Application
- Alias to Alias chat inside Restricted Areas
- Revocation removed from all credentials, excluding credSchool
- Inspection Application
- Tray Application for control of User Client status

The Restricted Areas functionalities were improved for the second pilot round, which included a bug fix, the addition of the Alias-to-Alias chat and a new layout of the whole application. Alias-to-Alias chat worked when the chat was enabled for the current Restricted Area and a certain user had clicked on another user's alias in the list of people who had entered the Restricted Area. This function allowed users to have private discussions without posting messages to a chat that would have been visible for all who had access to the Restricted Area. Technically, the chat function was the same as the one used to post to everyone, but with access restricted to two people/aliases.

Smart card initialization and download of credentials

For a successful start of the second pilot, EDOC prepared smart cards to be issued to all users that had signed the legal consent form. 34 smart cards were prepared for the first round compared to 381 for the second round.

Preparation of smart cards included the following steps:

- The customization of the smart card by printing was done using a special card printer. A smart card number and the ABC4Trust logotype was printed on all smart cards (see Figure 7)
- The installation of the ALU (adding the OS to the card using MUtil.exe)
- The initialization of the smart card to create a pseudonym and to generate the PIN/PUK codes
- The uploading of user data to the IdM Database, match the card pseudonym with the IdM record and save the user credentials prepared by the IdM Portal to the smart card

Due to the large number of participants in the second round of the Söderhamn pilot a decision was made that EDOC would download the credentials to the smart cards before handing out the cards to the users. This required that NSN had to add more functionality to the School Registration System. In the first round all cards were prepared by EDOC except for the last step which required the respective users to download their own credentials. In the second round EDOC made all the preparations and also downloaded the credentials. This added convenience comes at the price that the activities of the provisioner (EDOC) needs to be trusted



Figure 7: Smart card design

The teachers were the first group to receive their smart cards and card readers at the school. The teachers asked to have some time to familiarize themselves with the RA System and prepare some Restricted Areas to eventually be used by the pupils. The next group to receive their smart cards were the pupils. EDOC and SK administrators distributed the smart cards, PIN/PUK codes and smart card readers to the pupils in each class separately. The last group to receive their cards was

the guardians. The smart cards and the smart card readers of the guardians were given to the pupils to take home and give to their parents. The guardians received their PIN/PUK codes within a letter sent directly to their home addresses. The entire process was completed within 2 weeks.

New layout of the Restricted Area Application

The new layout of the Restricted Area Application included an effort to make scenarios and functionalities easier to understand. The design was also made to be in-line with current trends in general web layout and design.

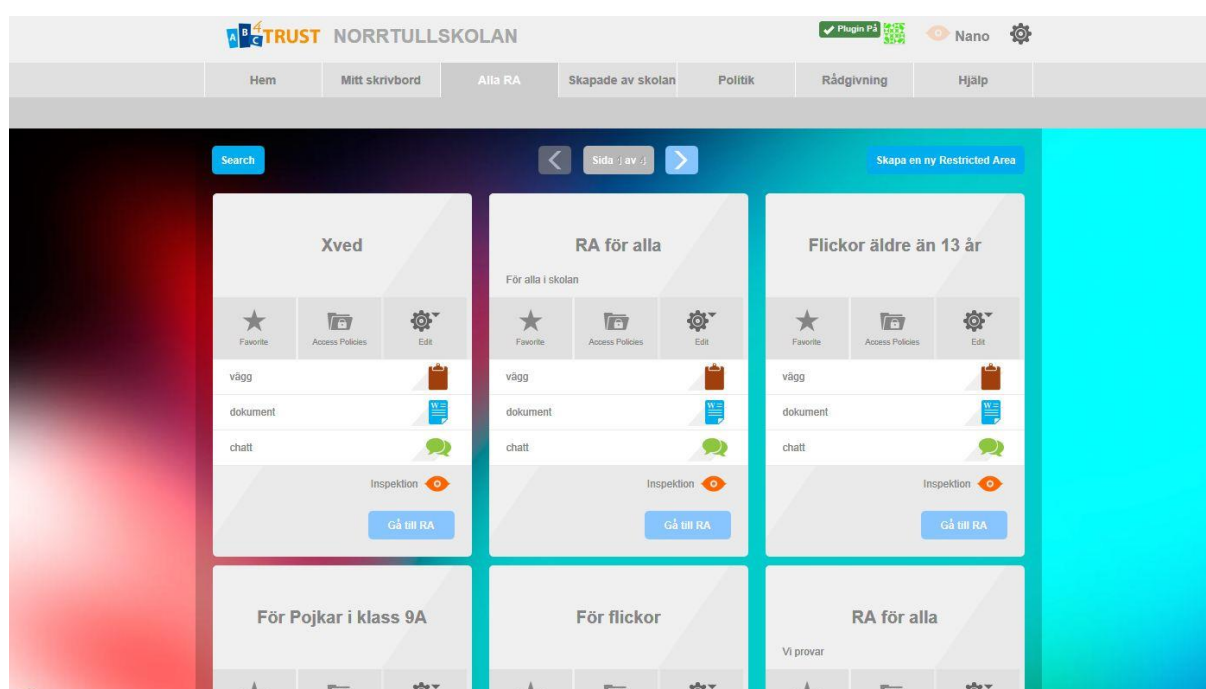


Figure 8: New Restricted Area Application layout

New Alias-to-Alias chat functionality

For the second round of the pilot a new functionality of Alias-to-Alias chat was introduced. The functionality allowed the users to start a chat communication session with another user by simply clicking on the alias of the user. The Restricted Area Application automatically created a Restricted Area and added the two aliases to the access policy so that they could chat privately. In this manner their conversation would not be visible to other users.

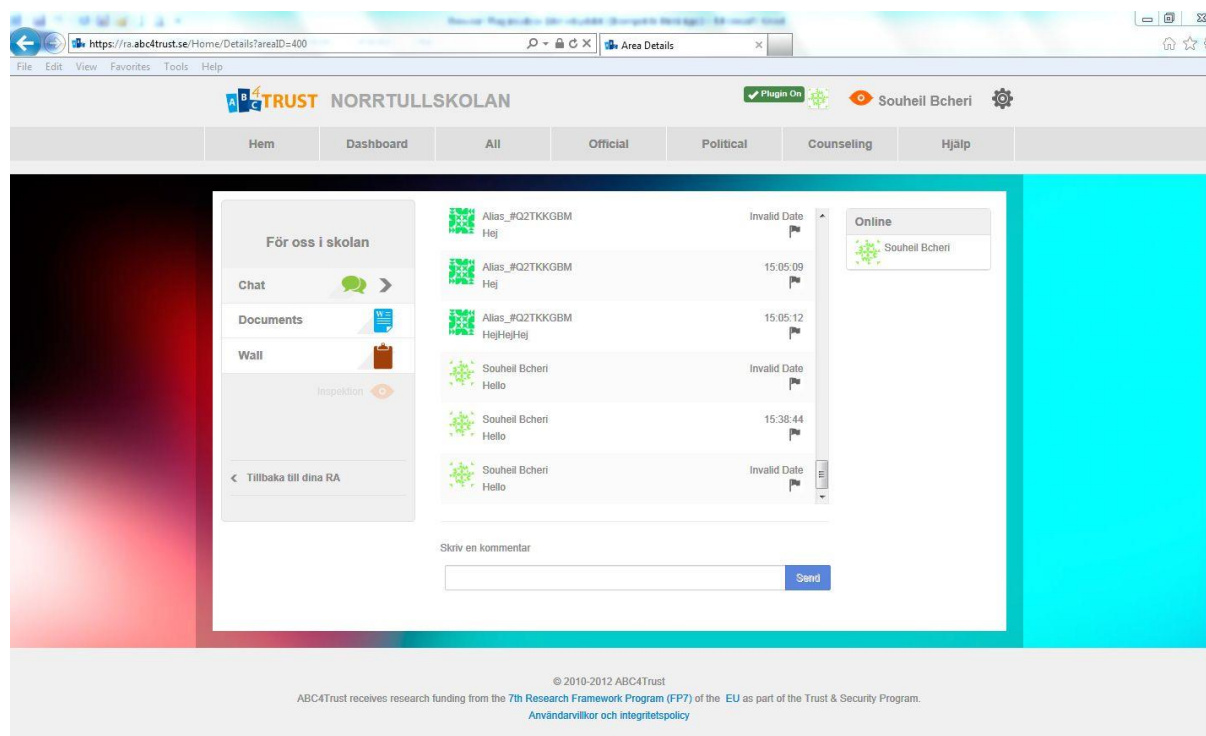


Figure 9: Chat in RA

Revocation

After the first round of the pilot it was decided to improve the performance of the entire system. Among improvements made, a priority was given to speeding up the login process when using the Restricted Area Application. This was accomplished by minimizing the number of controls (checks) towards the Revocation Authority in the following way:

1). Revocation (the revocation handle) was removed from all credentials except for the main credential, credSchool.

2) To assure that revocation control could still take place, a default access policy was added to all Restricted Areas that required the school name to be equal to Norrtullskolan.

Since this access policy was added to all Restricted Areas it guaranteed that a revocation check was performed whenever a user was trying to login at any Restricted Area and ultimately allowed for a more optimized system with a more efficient login process.

Inspection

The Privacy-ABC inspection functionality was introduced in the second round of the Söderhamn pilot to guarantee the physical and mental safety of each participating pupil. Since the inspection process provided a means to reveal the true identity of posters, it was used with great care and within regulations. More specifically, inspection meant the revelation of the pupil's identity could occur in certain predefined emergency situations (called inspection grounds). Such inspection grounds were concluded to be:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person.
- Situations demanding an intervention according to the Norrtullskolan policy against discrimination and degrading treatment.⁴
- An existing court order or other administrative request binding for Norrtullskolan or Söderhamn Kommun

The user was always able to see whether a Restricted Area was inspectable due to the presence of an indicator within the display and the word "Inspection" beside the indicator (see Section 5.3). In the event where a participant (pupil, legal guardian, or school staff) reported an emergency situation, an assigned School Inspection Board would investigate the matter. This board would decide if inspection was required by comparing the inspection grounds embedded into the presentation token with the current situation. In case the comparison was positive, the School Inspection Board triggered a formal inspection process by forwarding the request to an assigned Inspector. This Inspector would then perform a double check and was equipped with the technical capability to reveal the identity of the pupil. The whole process was also protocolled in order to guarantee that no single entity was able to arbitrarily spoil the privacy of the pupil and that the identity could be revealed only within the situations of the inspection grounds listed above.

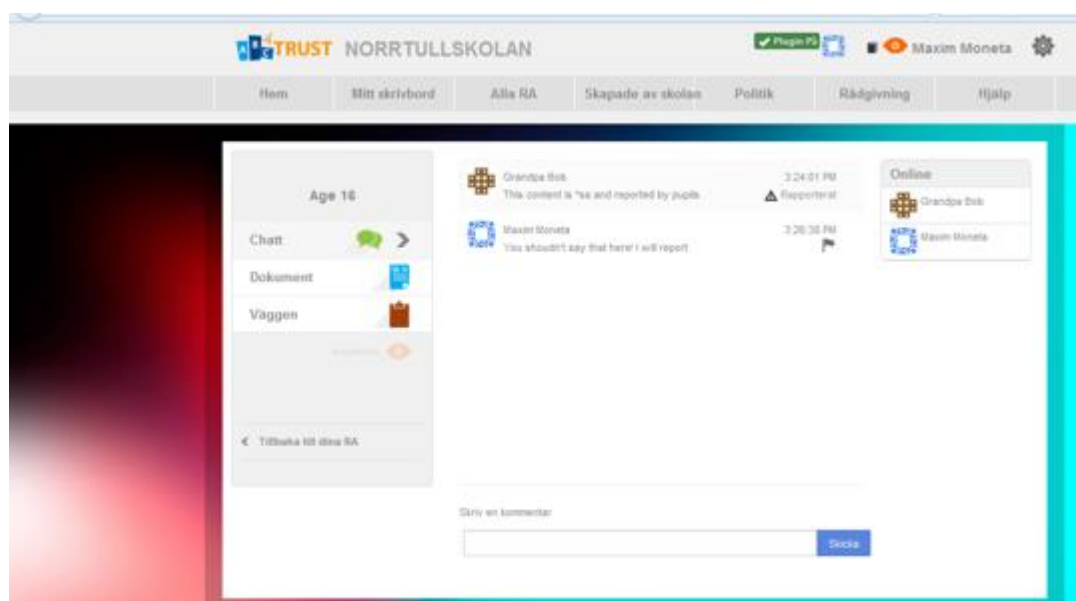
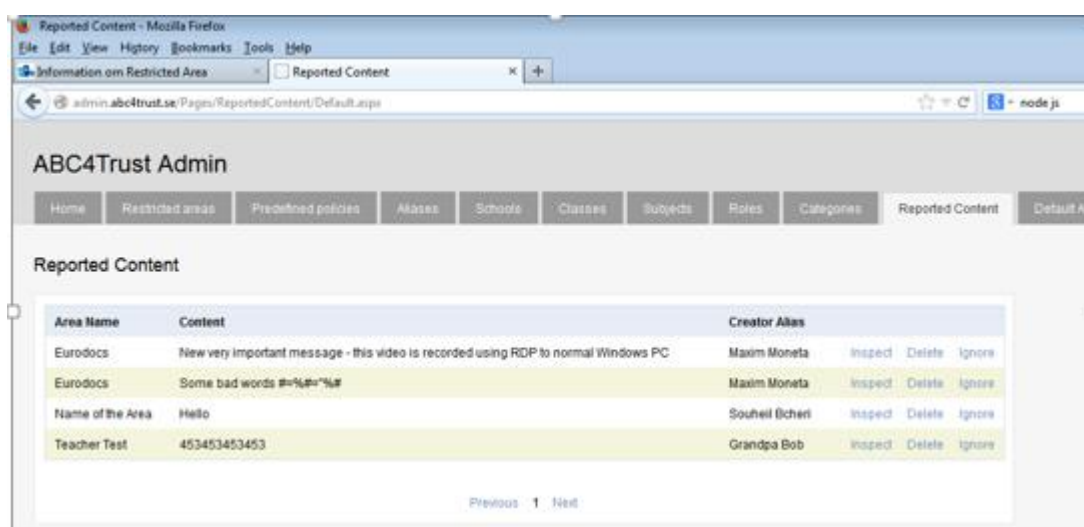


Figure 10: Reported message in chat

⁴ This policy can be found at <http://bit.ly/1e7ptSm> for further reading.

This process is initiated when an emergency situation occurs that causes the Restricted Area Application and the School Inspection Board to start the inspection procedure for a particular communication. An Inspector, with approval from the Inspection Board, can then reveal attributes from the presentation token stored with the communication. In the event where the School Inspection Board were to decide that the situation did not require the identification of the user, it either closed the case or could decide to delete the content and/or write a warning to the respective Restricted Area. Regarding more detailed explanation refer to Section 5.3.

Inspection was performed using the Inspector Application, a separate client application that is not connected directly to the Restricted Area database. The School Inspection Board has access to the list of reported content in order to be able to make a decision whether the inspection ground has been fulfilled or not. The inspection itself is performed only after such a decision has been made.



Area Name	Content	Creator Alias	Inspect	Delete	Ignore
Eurodocs	New very important message - this video is recorded using RDP to normal Windows PC	Maxim Moneta	Inspect	Delete	Ignore
Eurodocs	Some bad words #=%#=%#	Maxim Moneta	Inspect	Delete	Ignore
Name of the Area	Hello	Souheil Bchari	Inspect	Delete	Ignore
Teacher Test	453453453453	Grandpa Bob	Inspect	Delete	Ignore

Figure 11: School Inspection Board view

Function wise, the introduction of the Inspection process was the biggest change in the second round compared to the First Round. This covers both the amount and complexity of scenarios implemented as much as it does the perspective of software development.

Tray Application

Pupils in the pilot were primarily using the school's computers (laptops) to log into the Restricted Area Application when they were at school. Since those computers may have had many other programs installed, pupils sometimes complained about the school computers being too slow. This was also the situation before the pilot started. During the first round of the pilot, after the User Application was installed on the school computers it was difficult to verify if the computers became even slower because of the User Application or whether it was due to the other programs installed on the computers.

In order to isolate this performance problem and to improve the overall user experience while simplifying the process to debug problems, the decision was made to develop a Tray Application. The Tray Application, introduced in the second round of the pilot, was a Windows program that could be installed on the computer to act as a tray icon (indicator). This showed the status of the User Application while offering additional functionalities such as starting, stopping or restarting the local services. The Tray Application was also designed to be used to launch updates of the User Application.

3 Evaluation of School Pilot's Deployment

In summation, the two rounds of the Söderhamn school pilot were successful. The goals of successfully deploying the new cryptographic architecture and showcasing the Privacy-ABCs technology features, as well as the Restricted Areas application, were achieved. Moreover, the technical issues that arose during the first round of the pilot were successfully mitigated for the second round. Additionally, the overall improvements to the efficiency of the system made for a much more user friendly experience while adding an extra layer of improved administrative capabilities during the second round.

As a result of Swedish media's interest for the Swedish pilot a 2 minutes long TV-interview was broadcast during prime time news on Swedish national TV. The interview can be seen at the following URL: <http://bit.ly/1gHgd23>.



Figure 12: Swedish pilot on the Swedish national TV

3.1 Requirements and Fulfillments

The school pilot should provide end users with the following functions for community interaction, as specified in [BGL+12]:

- Counseling – counseling functionality developed according to the requirements and the database was filled with participating predefined counselors
- Restricted chat rooms – enhanced for the second round to let the pupils use chat and other Restricted Area functionality like walls with more comfort and better user experience, requirements fulfilled
- Political discussions – provided with no scenario changes from the first round, only general layout and functionality of modules changed, requirements fulfilled, but this item is more like a logical or virtual addition to general RA functionality which doesn't necessarily change the overall scenario of use

- Sharing documents – requirements fulfilled since this functionality was enhanced in alignment to changes made in chat rooms and walls
- Emergency situation measures – inspection application, school board interface and front-end controls to report content were on place and functional, requirements for functions fulfilled

Within the pilot, the following community functions have been evaluated:

- Public chat within Restricted Area
- Sharing documents within Restricted Area
- Wall posts within Restricted Area
- Chat within a Counseling session
- Alias to alias private chat

In the following list, we provide the predefined generic requirements which will form the core elements of the common generic requirements.

- Every user must be provided with a smart card reader and a corresponding PIN and PUK code.
- Revocation of Privacy-ABCs must be enabled by Privacy-ABC technology.
- Privacy-ABCs must be able to be bound to the smart card and/or to the user. During the issuance of Privacy-ABCs, the new credential must be able to be bound to a user in such a way that this credential would be deemed to be useless if transferred to other smart cards.
- The user must not be able to manipulate the presentation tokens or the Privacy-ABCs without damaging their integrity.
- The Privacy-ABCs must be stored on the smart card.
- Issuance token generation or a presentation token must require a PIN in order to authenticate the user.
- The user must be able to read all contents of her smart card except the user's secret (the latter requirement is provided as a built-in feature by the smart card).
- The user must be able to change the PIN of her smart card.
- The user must be able to unlock the smart card by entering a PUK (similar to the mobile phone handling).
- All processing of personal data requires a legal basis. Unless this is provided by law, informed consent of the participants is required.
- A presentation token must be non-linkable to the Privacy-ABCs which have been used to generate it, if the user chooses to remain anonymous.
- During the issuance of Privacy-ABCs, the new credential must be able to contain attributes from Privacy-ABCs already owned by the user without the Issuer being able to know the value of these attributes, i.e. carry-over attributes.
- Both the verifier and the issuer must be able to require the user to insert a pseudonym in her token bound to the user's secret such that the recipients of the token (Verifier and Issuer) can be sure that no one else other than this specific user can generate the chosen pseudonym.
- The user must have the possibility to generate a token with a specific pseudonym previously used by her.
- Both the verifier and the issuer must be able to require the user to insert a pseudonym in her token, which is not only bound to the user's secret, but also bound to a scope (a URL). In this special case, the Privacy-ABC technology must force the user to generate the same pseudonym (scope exclusive pseudonym) if the scope is the same.
- The Privacy-ABC technology must enable all players receiving tokens for checking if the tokens are based on attributes of Privacy-ABCs owned by the users sending the tokens.
- A replay of the same token must not be allowed by Privacy-ABC technology.
- Log files must be generated by the ABCE System, which will provide input for forensics and liability issues.

- The log files must never reveal the values of non-public keys and secrets.
- The user must be able to generate presentation tokens based on Privacy-ABCs, which were issued by different issuers.
- When the pilots are over, it must be possible to delete all the data stored about the users in the system (including the smart cards).
- Personal data must be deleted once it is not needed anymore. For this, deletion periods and a deletion process must be defined.

3.2 Specific Considerations for the Second Round

An important change in the second round of the school pilot was the introduction of inspection as a new feature.

Inspection grounds can be defined as the reasons for revealing the real identity of a pseudonymous user by decrypting the inspectable presentation token which includes the identity cryptographically hidden. Consequently, during the inspection the request for inspection and the correlating scenario have to be reviewed with regard to their accordance within the inspection grounds. Different Privacy-ABCs systems will include different inspection grounds, since they have to be adapted to the relevant use-case. However, in most cases a common inspection ground will be a legally justified demand of a third party such as a law enforcement authority. Within the Söderhamn school pilot, inspection grounds would be determined by the School Inspection Board.

The inspection is performed after a decision of the School Inspection Board. Technically, it consisted of EDOC retrieving an inspection token from the server and turning it over to the Inspector. The Inspector uses her special inspection application to inspect the token, and can thus reveal the identity of the person who posted the content associated with the token.

3.3 Statistics

The statistical results of the second round of the pilot confirmed that the natural growth of usage of the system coincided with the growth of the quantity of users. This led to more Restricted Areas, of more different types, being created (see Table 1).

Restricted Areas	Value for 2nd pilot	General Description
Total Areas	115	Total number of Restricted Areas created by users, including Private Restricted Areas.
Private Areas	40	Number of default RAs created automatically the first time a user signs in successfully using a default alias.
Pupil Private Areas	29	Number of restricted areas created by pupils and/or guardians.
Official Areas	29	Number of restricted Areas created by school personnel using the default alias and marked as official.
Counseling Areas	10	Number of restricted Areas created for counseling sessions by request of the user
Private Chat Areas	7	Number of instances where the user requested one-to-one communication with another user by alias.

Table 1: Restricted Areas created in second round

For the usage of this Restricted Areas users have created different aliases. The actual Default Aliases was reported as to be 381, whereby 889 was the total number of possible default users that were reserved prior to the start of the pilot. The amount of actual Default aliases differs to the

number available due to the fact that not all of them signed the consent form (see Table 2). Of these, 40 users successfully logged in to the Restricted Area Application at least once to use their default alias. Finally, a total of 108 aliases were created by the users in addition to the primary alias the user had been initially assigned.

Alias Types	Value for 2 nd pilot	General Description
Default Aliases	381 (889)	The default alias was the alias booked for a user before the pilot started and was kept in the application database to be handed over to the user on their first login to the system in conjunction with the confirmation of the user's real name and surname. Additionally, the default alias was used by school personnel to send official information privately to pupils and parents.
Used Default Aliases	40	Number of default aliases that were actually used by users.
Created Aliases	108	The actual number of aliases that users have created manually using the Alias Selector.
Anonymous Aliases	62	The number of anonymous logins to the system when a user selects the predefined alias "Anonym" in the alias selector.

Table 2: Aliases used in second round

Additionally, it is important to mention that, just as in the First Round, the option of using anonymous alias, where a pseudonym was created and saved in the database, was used quite often with regard to the quantity of anonymous aliases per active user – for the Second Round it was 62 aliases, which averaged out to be 1.55 anonymous aliases per user. If a user was logged in anonymously will not see her private restricted area and would need to switch alias.

Over the course of the pilot, users generated over 900 different forms of communication within the Restricted Areas, including chat messages, wall posts, political discussions and/or document uploads (see Table 3).

Communication Form	Value for 2 nd pilot	General Description
Chat Messages	850	Total quantity of messages from the chat functionality within all types of Restricted Areas.
Wall and Documents	52	Wall posts and document uploads to Restricted Areas of all types.

Table 3: Content in Restricted Areas

3.4 Evaluation of School Pilot's Network

During the first round of the pilot response times and set up of school's network satisfied all the requirements and did not affect the flow by any significant network delays.

One reported and solved case was the firewall rule which prevented EDOC from gaining access to the IdM Admin GUI using remote administration tools from school premises. After the issues were solved they did not affect the run of the pilot.

The second round of the pilot did not add anything to the previous findings regarding the network. The larger amount of traffic during the second round did not make any significant changes to the response times observed.

3.5 Evaluation of School Pilot's Services/Applications

For the first round of the School pilot applications were deployed using installers containing all the binaries packaged. This way of installation created a situation where it was necessary to track which actual version of client was installed on which computer and manually reinstall them in order to update. The initial installation process required local administrative rights on each computer and was considered easy to perform from scratch by the user, while updates could be made only with support from EDOC. Since the pilot users were performing testing and tasks only on school premises, this did not cause any problems in the first round.

To avoid a similar need for update support for the second round, the installer was enhanced with an update feature that allowed the user client installer to download the bulk update file from the Internet. The Installer then took this file containing all the needed components and automatically extracted them to a working directory.

Testing within the first round also discovered some problems with the client software, such as freezing of service and not implemented predicate. Since it was difficult to diagnose the nature of some hanged installations and failures during the first round, a tray application was added by EDOC prior to the second round of the pilot. The problems were documented and bug fixes were then implemented for the second round. The tray application was used to launch and stop services, as well as to retrieve the actual status of the User Client behind the Windows service. There were no reported cases concerning freezing of services during the second round of the pilot. As a result it was not possible to add administrative rights to tray application without opening potential risks to computer security. Controlling User Service was not possible otherwise, but once the user launched the installer again, rights were granted and the User Client was updated. This feature was used only during the testing stage prior to the second round start and did not have cases reported by users which would have required an updated User Client.

3.6 Evaluation of Smart Cards and Readers

Smart cards were utilized in the pilot in such a way that the user inserted her smart card into the reader which was connected to the PC.⁵ The user then navigated to the School Portal and clicked on the "Go to the Restricted Area Application". After this a new window would pop up asking the user to enter her PIN-code, which would allow the RA Application to communicate with the user's smart card. If the user entered the correct PIN-code the RA Application could begin communicating and interacting with the smart card, which included the smart cards operating system as well as the Privacy-ABC components that were stored on the smart card.

During normal operation of the smart card, which in this case means operations such as entering (log-in to) different Restricted Areas and conducting chat communication, counseling etc., non-

⁵ No contactless smart card readers were used in the Söderhamn pilot.

revocable credentials that resided on the smart card did not change⁶. The credentials could only be changed using the School Registration System (the Issuer).

The RA Application made use of aliases that were stored on the smart card as a way to avoid linkability. This means that the content that resided on the smart card did change during normal operation. This would only happen when the user created a new alias. Even though there was a limit in the card memory space where the aliases were stored, there were not any reported problems from any users regarding a lack of space on the card.

Storage space on the smart card was large enough to accept all the credentials needed for the first round, but this was achieved by decreasing the quantity of all the credentials and optimization of the credentials' size. Also, the credential specifications had to be changed to have one credSubject with all the actual subjects as attributes instead of creating a separate credential for each subject. The same was done with the credential credRole.



Figure 13: Smart card and card reader

In the first round of the pilot, there was a problem with respect to the ABC Engine (ABCE) getting the driver to release the lock on the card so that the U-Prove service could obtain the lock on the card when it was needed. This should be fixed with the introduction of an update to the PCSC (smart card integration) driver for .NET. This problem was solved before the second round of the pilot, and did not reoccur during the second round.

⁶ In the Söderhamn pilot, only the school credential is revocable. So in case the user loads new revocation information, her school credential will be updated but the attribute values of this credential will not change. Non-revocable credentials will not change even if new revocation information is downloaded.

During the first and the second rounds of the pilot the smart cards were working with no failure reports. All reports coming from the users during the operation phase were related to problems such as resetting of the PIN code and other functions not classified as failures of the smart cards.

With respect to the smart card readers, all the readers that were used operated as they should with the exception of one card reader from the first round that was most likely broken on delivery and was promptly replaced. Out of the 40 card readers that were tested, only one was not working. This means 2.5% of the card readers had a malfunction in first round. No malfunctions were discovered regarding cards and readers during the second round.

3.7 Evaluation of School Pilot's System Security

During the time periods the first and second rounds of the pilot were running no security issues were observed or reported, nor had any security related incidents occurred.

The first round of the school pilot included basic testing of different smart cards used with the same laptop as the part of several use cases. Since all users were tested using the same set of school laptops, this was only done with the standard school laptop configuration. The second round of the pilot included usage of home computers in addition to the school laptops. The introduction of new computers to an established system provided additional risks as the potential for security issues rose dramatically, however, no additional security lapses were detected.

As mentioned above, we had no reports of security problems with any of the components of the pilot. However, after the first pilot all the scenarios were reviewed by the partners and common discussions took place to eliminate possible risks. To provide security and avoid linkability during anonymous sessions the dashboard made separate requests to the database for each alias. Each time a user switched aliases the previous session was ended and a new session was started. Additional layers of security within the structure included the issuance of session tokens and the use of the non-replayable https. No security problems were discovered.

3.8 Evaluation of School Pilot's Availability

During the first round the servers running Restricted Area Application, School Registration System and all needed server components were available 24/7 and no crashes or downtime were reported, with exception to small maintenance breaks for updates which were not intersected with the testing schedule of the pilot.

During the second round there was a problem with Verifier not starting because of U-Prove path after a scheduled reboot of the server. The problem was reported, localized and auto-start scripts fixed. This problem did not reappear after that.

3.9 Evaluation of School Pilot's Response Time

The component response times satisfied the needs for the first round run in that the users did not report significant delays in response time. However, EDOC collected user feedback and noted that some improvements could be made. Among noted improvements there was an optimization of the revocation section, significant performance improvements for the User Client and a set of changes for Restricted Area application.

The stress test done with users within the first round proved that the response times were enough to provide a possibility for collaboration between a set of users in the same Restricted Area. Table 4 shows measurements collected with users running the system. The table presents rough measurements that were collected at run-time. Time was measured and is given in seconds. The measurements included two main cases:

- Case 1: Login to RA Policy, Not equal-to birthdate with inspection

- Case 2: Login to RA Policy, Not equal-to birthdate without inspection

Process	Case 1 (Inspection)	Case 2 (No Inspection)
Generate XML Policy (RA, Verifier, RA)	3	3
Create presentation – UI compares policy with user’s credentials	7	7
Share UI	1	1
Generate presentation	12	8
Verify presentation	4	2.3

Table 4: Measurement of timing (all times are in seconds)

According to results shown in Table 4, inspection added 4 seconds to the process of generation of a presentation token and 2 seconds to the process of verification of the presentation token.

In Table 5, we provide some measurements of the time used for the operations on the smartcard during presentations and issuance. The PC handling the smart card caches some data the first time the smart card is used which makes the following operations faster, so both times with and without cache are provided. These tests were conducted on a 2.2GHz Duo Core PC running Windows 7 using the “Teo by Xiring” card reader, the same card reader that was provided to all participants in the pilot. The timings differed with different policies, and due to the fact the users had the option of creating very complex policies, we were unable to conduct and present timings for all conceivable possibilities, so we present two different presentations in Table 5. Table 5: Performance Measurements

	1024 bit		2048 bit	
	<i>Without cache</i>	<i>With cache</i>	<i>Without cache</i>	<i>With cache</i>
Presentation involving two credentials	10 s	7 s	15 s	9 s
Presentation involving one credential with inspection	8 s	5 s	10 s	7 s
Issuance of one credential	8 s	7 s	12 s	11 s

Table 5: Performance Measurements

3.10 Evaluation of the Restricted Area System

The Restricted Area System consists of the following three main components that are evaluated: Restricted Area Application, School Portal and Tray Application.

Restricted Area Application

During testing and the operation phase of the first round it was hard to debug problems. This was due to the fact that it was difficult to isolate the problems in order to know if the problem was caused by the Restricted Area Application itself or by any of the other applications. Prior to the launch of the second round of the pilot the logging functionality of the User Application and the Restricted Area Application were significantly improved and debugging became more efficient.

During operation of the second round the Restricted Area Application served the users well and no known issues or problems were discovered by EDOC or reported by the school or by the pilot users. Users were able to use the Restricted Area Application in the way it was intended to be utilized. Teachers could create Restricted Areas and define access policies while the pupils could enter different Restricted Areas and post/receive messages and documents.

School Portal

The School Portal was utilized in two different ways during the two rounds of the pilot. In the first round the users received their smart cards that was initialized and prepared but did not contain the credentials. Each user had to visit the School Portal and navigate to the IdM Portal in order to download her own credentials.

In the second round this was changed. EDOC initialized and downloaded all needed credentials to the smart cards before they were handed over to the users. So there was no need for the users to visit the IdM Portal. The link to the IdM was not removed from the portal, however, in the event the user needed to download new credentials. This happened in a couple of cases when the name of one user was misspelled. The name was changed in the IdM Database via the IdM Admin Tool which automatically triggered the revocation of the old credential. A new credential was issued and downloaded by the user herself.

Not only the design of the School Portal was changed between the two rounds of the pilot but also the content such as the FAQ section, the user manuals and the links to the User Application Installer were all updated to reflect the latest changes in the system's development.

While the two rounds of the pilot were running there were no reports about downtime or unavailability of the School Portal. The School Portal has the built-in potential serve a much larger number of simultaneous requests than what was tested within the scenario of the pilot.

Tray Application

The Tray Application was installed on all laptops at the school and was mainly used at the start of the second round while testing and debugging the system at the school. The Tray Application, in combination with the User Application logs, helped in troubleshooting, localizing and solving some of the problems that were faced at the beginning, i.e. computer freeze and service hanging. The users did not use the Tray Application on their private computers at home. The Tray Application fulfilled its purpose and served the pilot well.

4 User Evaluation Results

This chapter focuses mainly on the results from the second round questionnaire. Section 4.1 gives a summary of the first round questionnaire results.

4.1 First round questionnaire summary

After the first round of the Söderhamn pilot was conducted, users completed a questionnaire. The results and the feedback from the first round were used not only to make technical improvements to the IdM, the User Client and the Restricted Area Application, but also to improve the pilot preparation process such as downloading the credentials to the smart cards before the cards were handed over to the users.

The first round of the Söderhamn pilot included the participation of 10 teachers and 22 pupils. Most of the users who received smart cards reported that they tried to use the system. Tasks provided by EDOC were performed by 68% of the students who filled-in a user report that was designed as a questionnaire (see Appendix A).

Additionally, a stress test was conducted where 8 pupils and 2 representatives from EDOC were logged in to the same Restricted Area and performed different tasks with the Restricted Area.

The most important findings of the first round questionnaire were that 73 % of the pupils found the Privacy-ABC technologies to be a good idea and in general had positive expectations on the potential (see Figure 14).

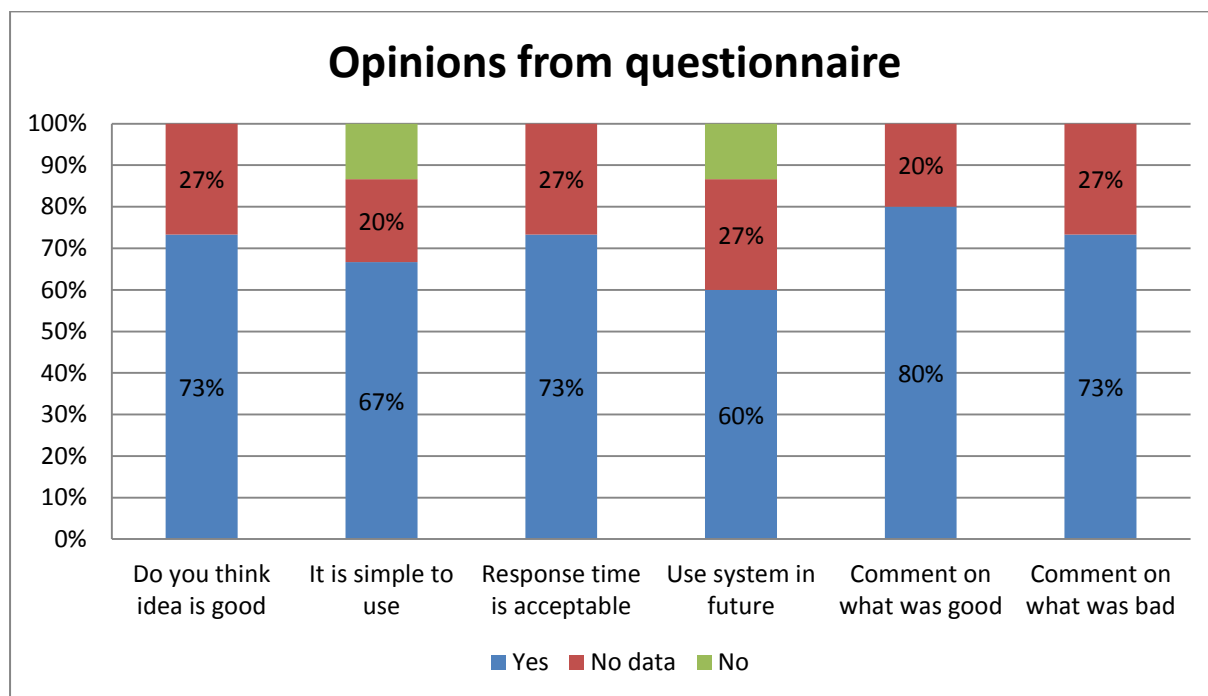


Figure 14: Opinion from the first round questionnaire

4.2 Evaluation of User Experience and Feedback

For the evaluation of the second round of the school pilot, it was decided to complement the statistics of the communication system with answers from the participants to a questionnaire. However, due to the fact that the majority of the participants were minors, careful consideration had to be given to the phrasing of the questions. 71% of the participants of the questionnaire were under the age of 18 and thus, the questions had to be adapted to their capabilities. Consequently, the age of the target group did not only affect the wording and the number of the asked questions but also the overall concept of the questionnaire, resulting in a need to create a shorter and more simplistic questionnaire. Therefore, the amount of questions was limited to 20 overall. Additionally, due to the complexity of the ABC technology and the concepts of privacy, anonymity and pseudonymity combined with the goal of not overburdening the participating pupils it was only possible to touch these subjects rather generally. The questionnaire was divided into two parts, with the first part focussing on directly pilot-related questions and addressing specific functionalities of the Privacy-ABC System. The second part of the questionnaire, however, concerned mostly the general conceptual understanding of the ideas behind Privacy ABCs. The complete questionnaire can be found in the Appendix A.3 User's questionnaire – Second round – English version.

Altogether 91 persons participated in the questionnaire and the exact statistical distribution according to age, gender and roles can be seen in the charts below.

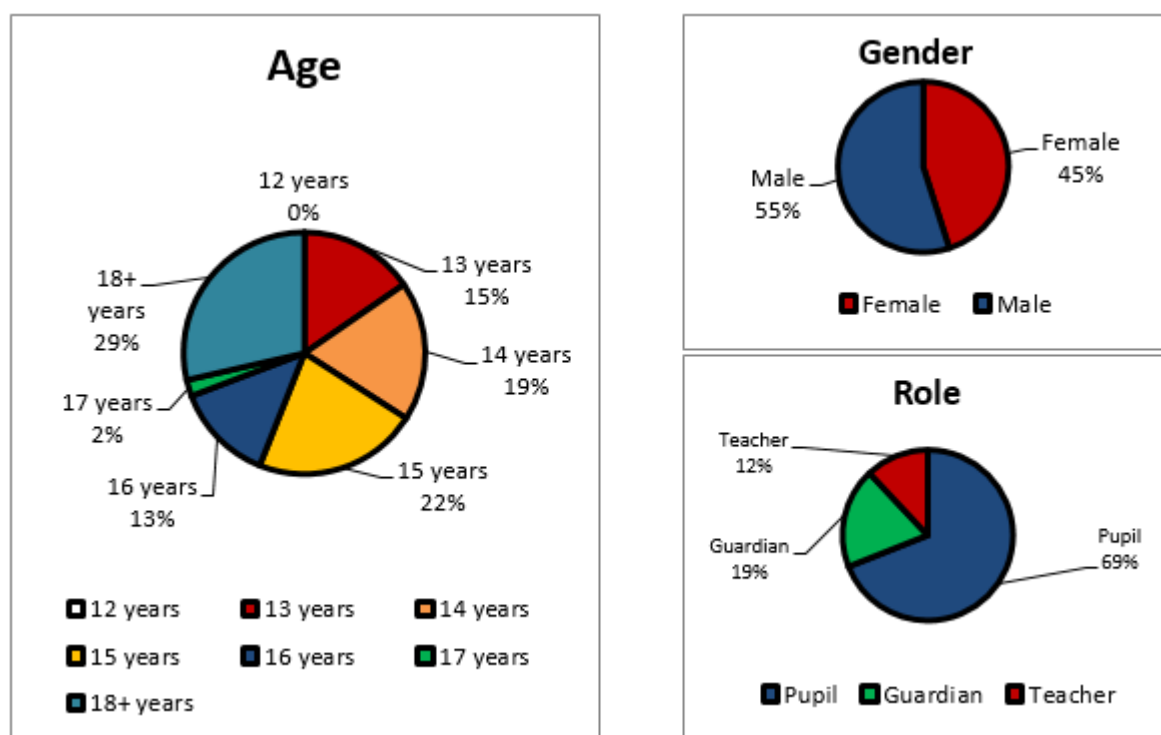


Figure 15: Participant Distribution

4.2.1 Functionalities of the system and their utilisation

The first group of questions which will be elaborated on in this subchapter covered purely statistical facts. They were meant to give feedback on which of the functionalities provided in the pilot system were actually used and with which frequency. The intention was to establish a statistical foundation for future Privacy-ABC research work and other developers implementing ABC technologies. Therefore, in the following paragraphs, the results of the separate questions

will be complemented with some considerations regarding the overall outcome of the questionnaire, the functionality itself and possible actions to increase the utilisation of the possible features.

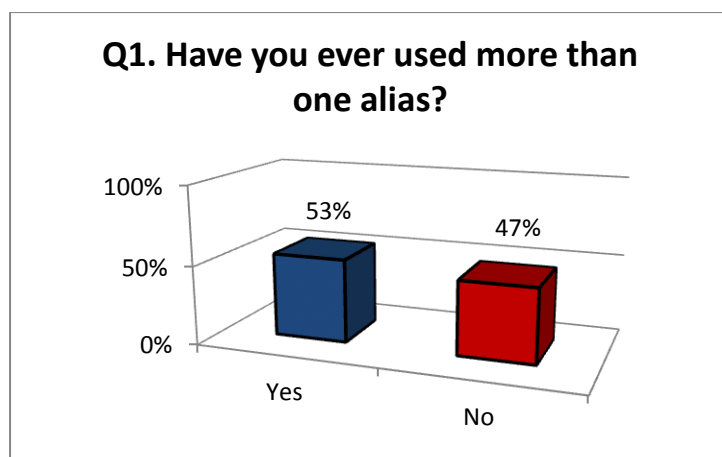


Figure 16: Results of question 1

The possibility to use more than one alias is one of the core privacy protecting features of the ABC-technology. The more information is disclosed under one alias, the easier it gets to identify the person behind the alias. Furthermore, if one alias would be inspected and revealed, all the associated information could be related to the real identity of the user. Therefore, it seems important to include the possibility that the same user can interact under different aliases. Nevertheless, during the pilot only 53% of the users took advantage of the given possibility. However, the statistics of the system show that the participants who were aware of this option used it quite frequently. While only 40 default aliases were used (initial alias with the real name of the participant), 108 further aliases were created. Furthermore, 62 times users interacted under anonymous aliases. Moreover, there are several aspects explaining the result of this question. First of all, 31% of the participants were teachers or parents mainly interacting in an official capacity. Consequently, for these participants there was no use for interacting under different names since they had to be identifiable in their capacity. Secondly, as the complete ABC-technology – the possibility to use a communication system under different aliases while staying logged in into the system was new and unknown to most participants. Therefore, it is not surprising that getting accustomed to this new feature would require some time. Nonetheless, it would be advisable for future developers of similar systems to advertise this feature to a greater extent than in the pilot, for example by a pop-up window suggesting the usage of a new alias at every log-in into the system.

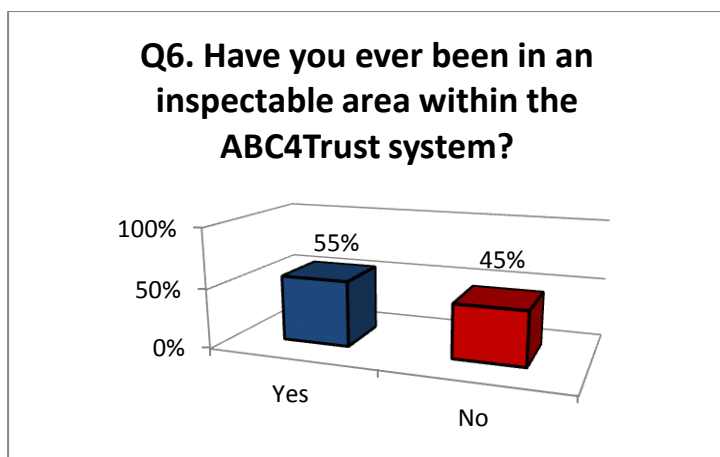


Figure 17: Results of question 6

Even though more than half of the participants have interacted in inspectable areas, the number still seems surprisingly low. Due to strict legal responsibilities and oversight obligations of the school for its pupils all but one (namely the Restricted Area for political discussions) of the Restricted Areas in the communication system were inspectable (see Section 5.3). However, the low number can be explained by the result of another question (Q7.) which showed that 35% of the participants were not aware of the fact that they were interacting in an inspectable areas (see below chapter 4.2.2). Therefore, it can be assumed that this lack of awareness led to the low number. Furthermore, the result is contradicted by the result of the following question (Q9). According to that one nearly two thirds of the participants used the chat function of the pilot system and since the all but one of the chat rooms – as parts of the Restricted Areas – were inspectable, these participants most likely interacted in inspectable areas. The satisfactory result of the latter question, however, appears even more so when correlated to the percentage of participating pupils (69%). The chat rooms with limited access for a certain group were mainly set-up for or by pupils. Therefore, it can be presumed that nearly all pupils entered a chat room at least once. Furthermore, 40% of the participants did not only enter a Restricted Area with limited access for a certain group but did even create an area on their own.

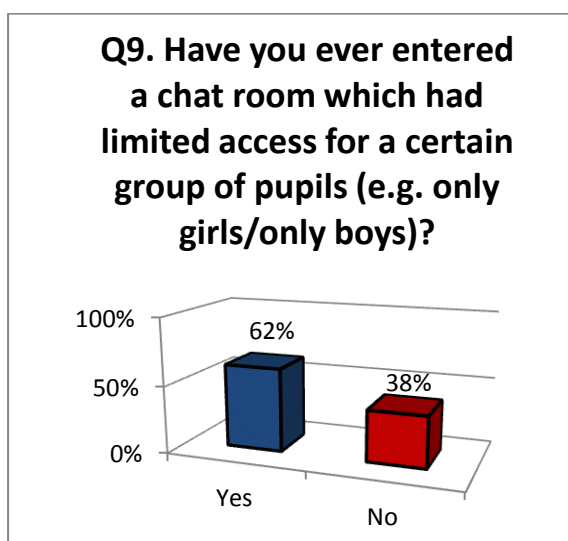


Figure 18: Results of question 9

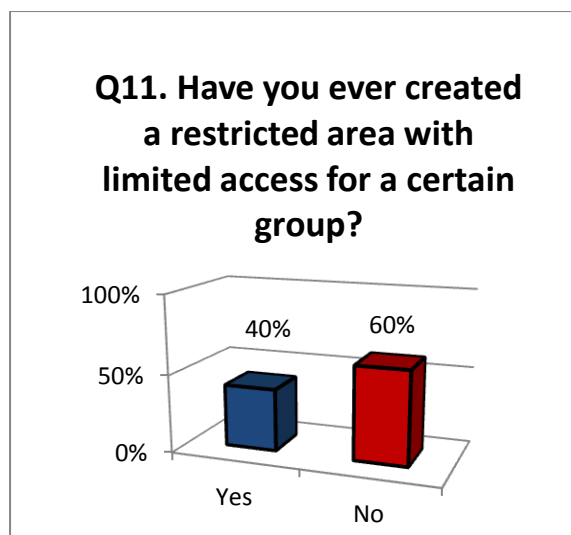


Figure 19: Results of question 11

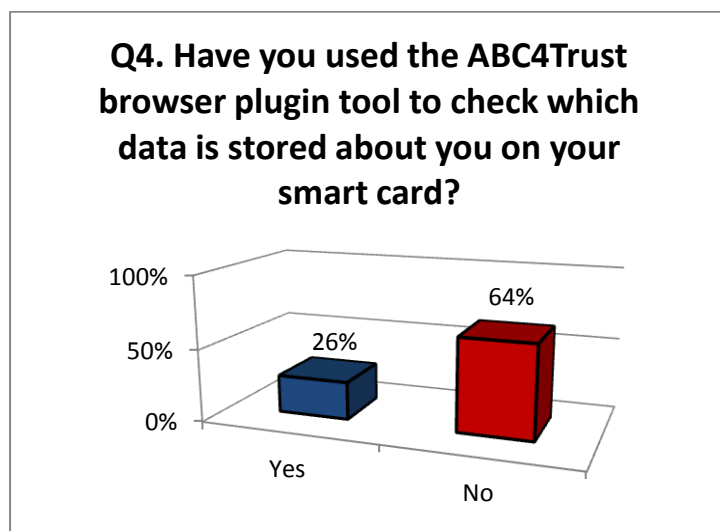


Figure 20: Results of question 4

26% of the participants checked which data was stored about them on their smart card. Even though this number may appear low at a first glance, it was in fact a very acceptable result. The browser plugin tool to check which data is stored about oneself was included to simplify the exercise of the user's right of access to stored data. Users' or data subjects' rights are mostly exercised by requesting the data from the data controller and therefore normally demand a lot of effort. Thus, it seems that by simplifying the procedure it was possible to motivate more participants to check their data and not blindly trust the ABC4Trust project and the ABC technology. In conclusion, more than a quarter of the participants being interested in their data and exercising their right of access is an unusual high number. This shows an increased interest of the pilot's participants in certain aspects of data protection, such as the scope of the personal data storage within the Privacy-ABC System.

4.2.2 Usability and Transparency

This subchapter will take a closer look at how transparent and user-friendly the pilot system was. In particular, the issue of transparency which had been outlined as one of the specific data protection goals in the previous deliverable [D6.1] is a crucial element of privacy enhancing technologies such as Privacy-ABCs. In this context, ‘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 (...).’⁷. Thus, usability is closely connected to the goal of transparency. Only if users can comprehend their interactions in the system, they can sensibly balance the benefits and disadvantages of disclosing information. In particular, in a system based on Privacy-ABC technology which enables users to disclose only a minimum of information, usability is of up most importance.

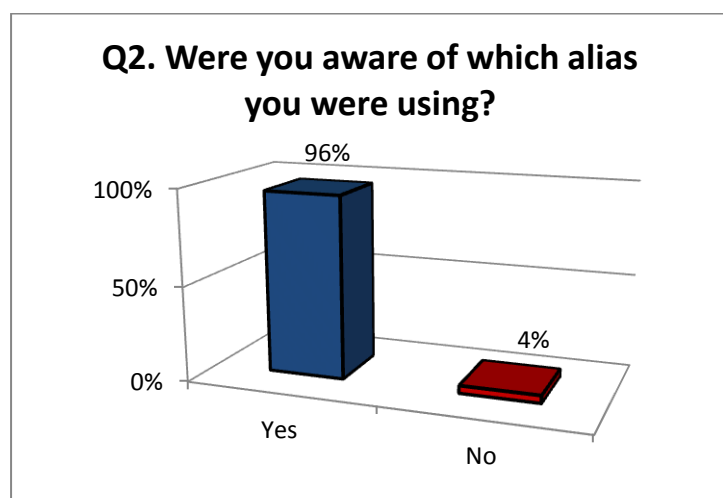


Figure 21: Results of question 2

Based on the previous question (Q1.) covering the usage of more than one alias this question enquired if users were aware at all times which alias they were actually using. To achieve and foster this awareness, a new feature was implemented showing the current alias in the top right corner of the User Interface (see Figure 22). The results showed that 96% of the participants who had used more than one alias were aware under which one they were currently acting in the school communication system. This shows that the display of the current alias worked well in enhancing the user awareness, making it transparent under which self-chosen identity the user was acting.

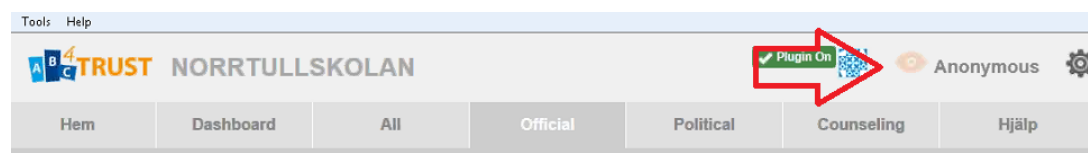


Figure 22: Screenshot to question 2

⁷ 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.

As mentioned before (see Chapter 4.2.1) the next question (Q7.) of the questionnaire showed that only 65% of the participants were aware of the fact that they were interacting in an inspectable area. This surprisingly low percentage was in particular unsatisfactory since it was linked to the interactions in inspectable areas and therefore with the most privacy intruding part of the pilot system. Especially in this context transparency would have been important because the inspection feature limited users to only pseudonymous interactions and allowed the revelation of their real identity. This low level of awareness proved an increased need for transparency features within the system. However, due to the importance of this issue it will be discussed in more detail in chapter 5.3.

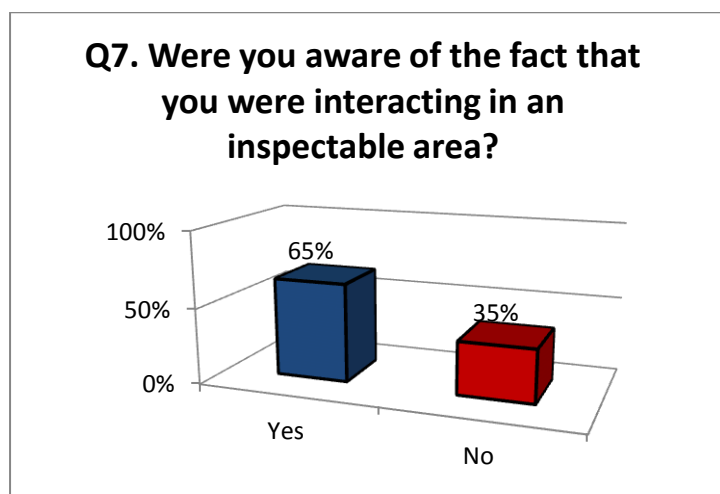


Figure 23: Results of question 7

4.2.3 Comprehension of the ABC system

The importance of transparency and usability in a privacy enhancing communication system has been explained in the subchapter above. Furthermore, it was explained that transparency in its core means comprehending the technical and organisational circumstances. Therefore, the questionnaire included two questions (Q3. and Q5.) examining the comprehension of two core features of the ABC-system – requesting a presentation token and entering a Restricted Area in compliance with the access policy. Interestingly, the results show that the percentage of correct answers nearly exactly coincides with the percentage of participating pupils.

The first question (Q3.) simulated the process of requesting a presentation token in the Identity Selector. During this process, the system discloses to the user which attributes are revealed in the requested token. In the screenshot of the question (see Figure 24), the only attribute required for disclosure was that the user is a pupil. The result showed that 69% of the participants chose the correct answer while 31% of the answers were incorrect. However, the high percentage rate of 31% false answers could be founded in a multitude of reasons. It may be that participants confused the terms “name” and “alias”, which might have led to the assumption that one’s name would be disclosed. An alternative explanation might be that the participants were uncertain about inspectable presentation tokens in general and which information is disclosed by them, since the example screenshot showed an inspectable presentation token. Nevertheless, the result shows that nearly one third of the participants did not fully comprehend the process of requesting presentation tokens. This encompasses in particular the knowledge which information would be disclosed in the tokens. The functionality of the Identity Selector is a central part of the Privacy-ABC technology used in the pilot. Due to this fact and regardless of any possible explanation of this result, it appears of utmost importance to improve the understanding on this matter.

Consequently, it is necessary to explore different ways of how to enhance the comprehension of the user, e.g. by providing further information in the User Interface or interactive tutorial features.

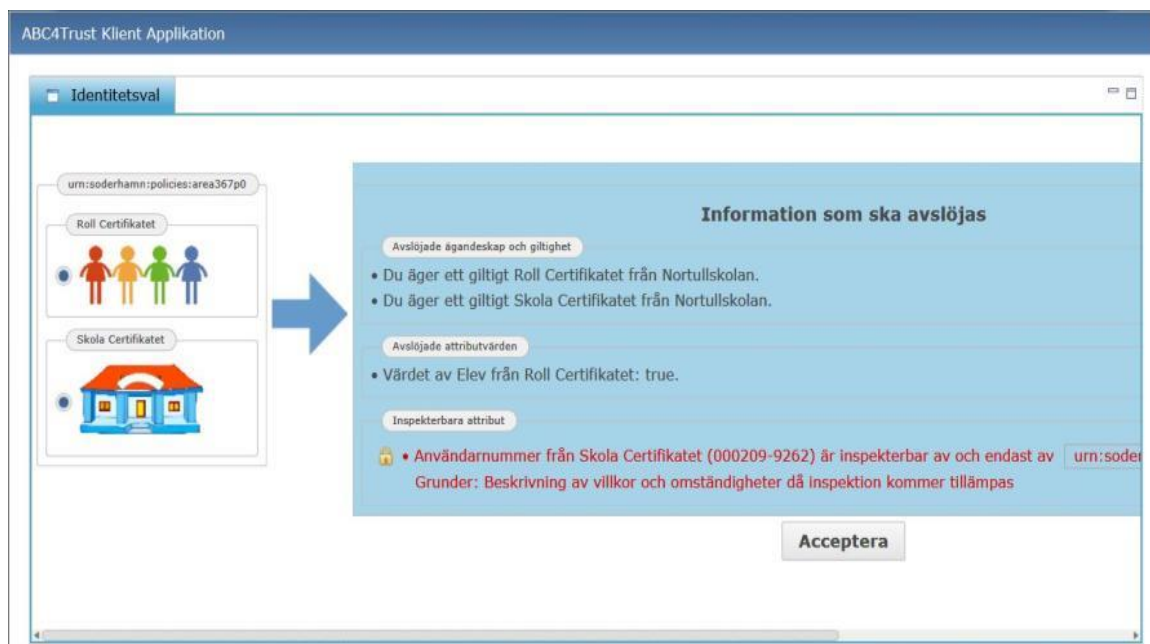


Figure 24: Screenshot to question 3

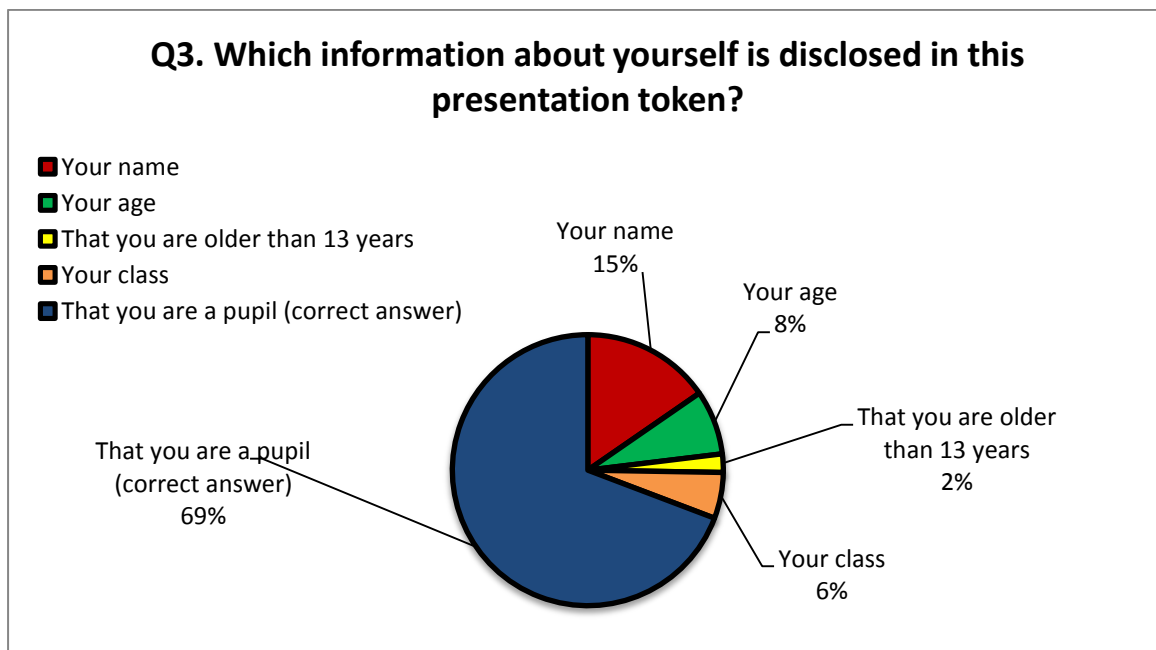
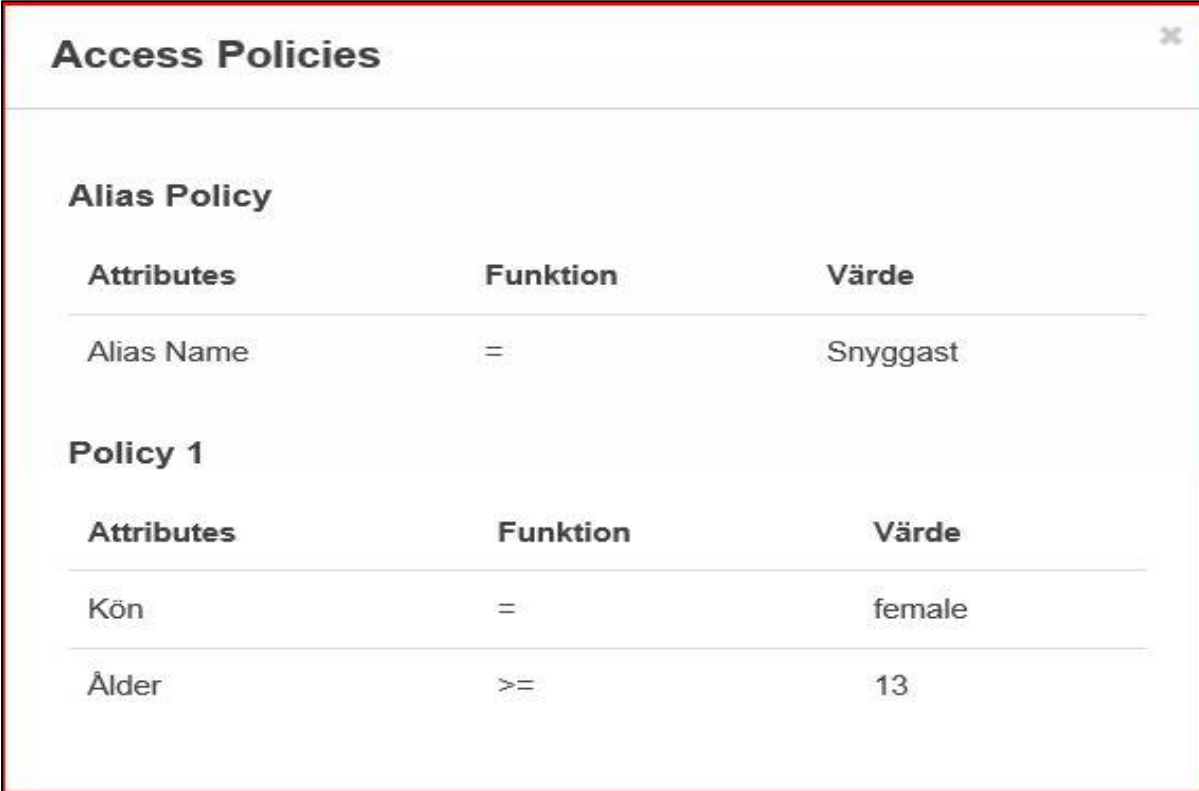


Figure 25: Results of question 3

In the second question (Q5.) entering a Restricted Area with limited access for a certain group – here all girls 13 years or older – was simulated. The necessary personal attributes for entering are outlined in the screen, showing the access policy (see Figure 26). Again in this question, over two thirds of the participants answered the question correctly. Additionally, 15% (11% + 4%) of the remaining responses were half-correct by selecting ‘all girls’, or ‘all persons older than 13 years’. Nevertheless, understanding access policies correlates directly with the permission to enter certain

areas and thereby with choosing the correct attributes in the Identity Selector for their disclosure in the requested presentation tokens. Therefore, it was desirable to achieve the highest number of correct answers possible. Similar to the previous question, the conclusion has to be that more information needs to be provided to the participants. Only thereby it can be achieved that the user fully comprehends the provided User Interface functionalities and the correlating conception of the Privacy-ABC technology.



The screenshot shows a window titled "Access Policies" with a close button (x) in the top right corner. It contains two tables of policies. The first table, "Alias Policy", has three columns: "Attributes", "Funktion", and "Värde". It contains one row: "Alias Name" with the function "=" and the value "Snyggast". The second table, "Policy 1", also has three columns: "Attributes", "Funktion", and "Värde". It contains two rows: "Kön" with the function "=" and the value "female", and "Ålder" with the function ">=" and the value "13".

Alias Policy		
Attributes	Funktion	Värde
Alias Name	=	Snyggast

Policy 1		
Attributes	Funktion	Värde
Kön	=	female
Ålder	>=	13

Figure 26: Screenshot to question 5

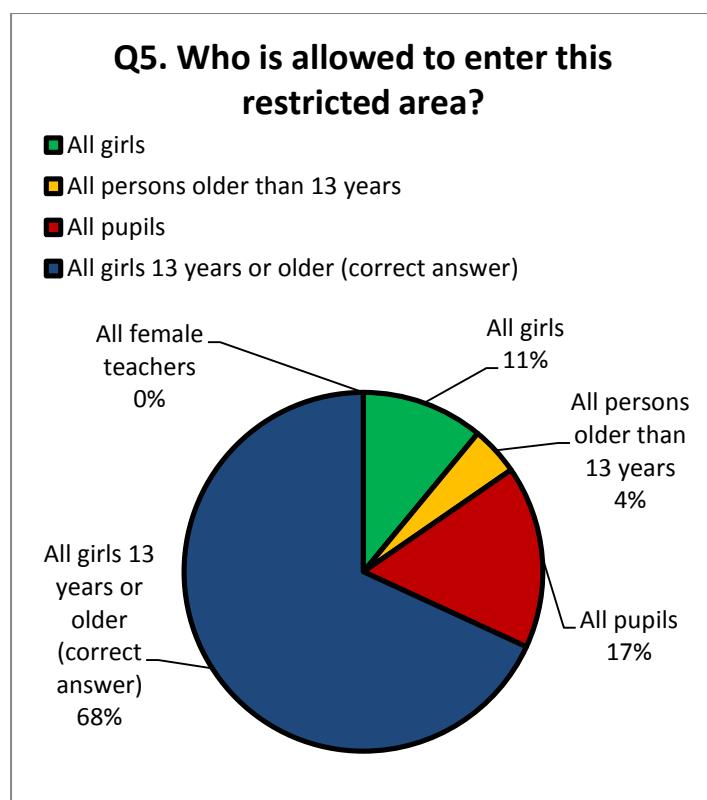


Figure 27: Results of question 5

4.2.4 Trust and Acceptance

The last set of questions (Q8., Q10., Q12., Q13., Q14.) in the first part of the questionnaire examined the trust of the participants with regard to specific functionalities of the ABC technology, the motivation behind the usage of those, and the general acceptance of the pilot system.

As mentioned before, the inspection function is one of the features in the pilot system worthy of further discussion. Therefore, it appeared important to find out the opinion of the participants about the inclusion of this feature. The inclusion of inspection constituted a balancing act between privacy protection and the protection of the school pupils in cases of emergency and unlawful user activities in the Privacy-ABC system. Consequently the general user acceptance of the inspection feature is a central subject of the pilot evaluation. The questionnaire showed that 79% of the participants who had interacted in inspectable areas felt safer because they knew that someone could assist in certain scenarios. Moreover, the result also proved that the participants trusted the school and the system administrator that they would comply with the stated regulations (in particular the pre-defined inspection grounds) and that the technical possibility of revealing their identity would not be abused. However, this result should not be generally transferred to other Privacy-ABC systems since the particular circumstances – a school in Sweden with mostly teenagers as participants in the pilot – have to be taken into account. In other settings, e. g. with older participants or different national backgrounds, the acceptance of the inspection feature might be different depending on the privacy concerns of the involved user group.

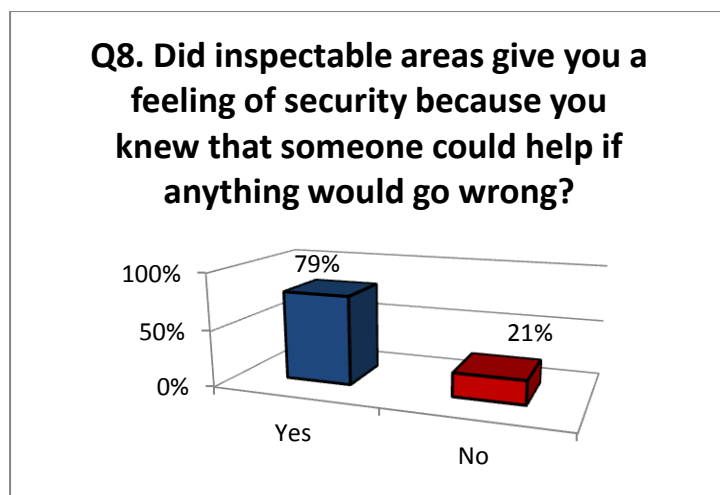


Figure 28: Results of question 8

A further sign of trust was the result of the next question. This time, however, the result showed that the participants trusted the Privacy-ABC system itself. 96% of the participants who had entered a chat room with limited access for a certain group were confident that all other members in this chat were also allowed to be there. Since the permission to enter is based on an automated decision at the core of the ABC technology, the result showed that the majority of the users trusted that the system is working without fault.

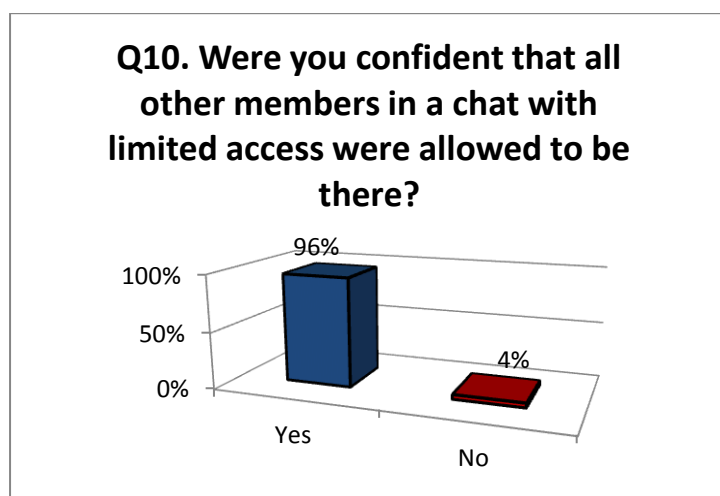


Figure 29: Results of question 10

The following two questions (Q12. & Q13.) correlated with the previous one. The idea behind the question concerning access without permission was threefold: First of all, a failed attempt to access a Restricted Area to which someone did not have access to, could elevate the trust in the system which was enquired about before. Secondly, since the participants were mostly pupils, the idea of trying to 'sneak' into prohibited areas seemed rather reasonable. Lastly, the first question had to introduce the second one. The second question, however, was important since the school pilot did not include any safeguards preventing pupils from swapping their smart cards – as the tombola in the Patras pilot (see [D73]) – and therefore it was interesting to know how many participants did swap their smart cards at least temporary. Technically, it was not possible that someone would enter a Restricted Area to which he/she should not have had access to due to wrong or missing attributes. Thus, it must be assumed that attempts to enter could have only be

successful with a smart card of someone else, or if another participant was already logged in into the system. The result revealed that around one third tried to access a chat room without permission and 13% of these claimed to have succeeded. However, while the percentage rate seems quite high it has to be mentioned that in this instance 13% is on par with 4 participants.

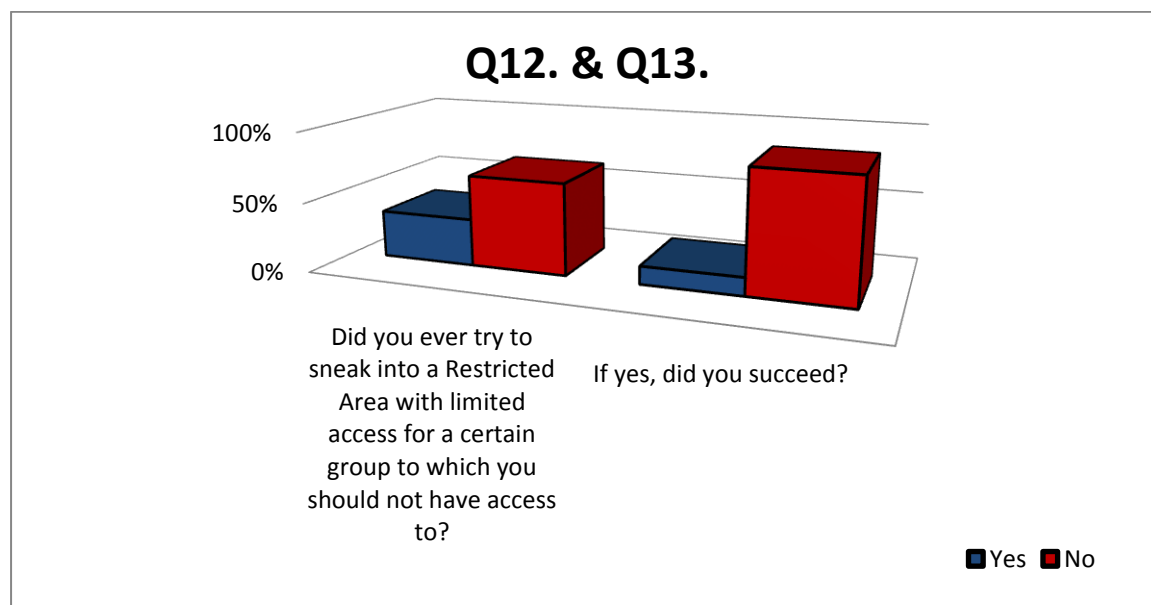


Figure 30: Results of questions 12 and 13

The last question of the first part of the questionnaire (Q14.) explored the preferences of the participants in regard to logins with password/username or the pilot system. The result of this question was significant for several reasons; firstly, from the beginning of the project it was evident that Privacy-ABCs would have to compete with logins by password/username. Up to now, the most common way of authentication or identification while surfing the internet is based on a full disclosure of one's identity at first and subsequent logins via password and username. With Privacy-ABCs, however, only a set of tokens and not all information about the user need to be disclosed. Therefore, a new way of logging in is available which is additionally exceedingly privacy preserving. Furthermore, Privacy ABCs comply with legal obligations concerning data minimisation to a greater extent. Nevertheless, a widely-spread introduction of Privacy ABCs will only succeed if they are commonly accepted by users. The second reason for this questionnaire inquiry was the fact that it allowed each participant to weigh the pros and cons for themselves and to come to a final consideration regarding the pilot system. While the previous questions aimed rather at possibilities to improve the Privacy-ABC system as used in this specific pilot setting this question ascertained the general acceptance of a new and unknown system. Furthermore, since the project pilots were the applied use-cases of this project, the answers of the participants were not based on pure theoretical considerations, but on hands-on experiences with a running Privacy-ABC system.

In the end, the questionnaire yielded a very sound result. 56% (28% + 28%) of the participants would prefer a login with the ABC system and only 16% (4% + 12%) would like to keep logging in with password and username. The remaining 28% were undecided. However, taking into account that it was a test pilot which could not show all the capabilities of Privacy-ABC technologies due to factual, organisational and legal restrictions in this project, it appears likely that the majority of the undecided users could be convinced of the benefits of a Privacy-ABC system. Consequently, a second improved pilot and further research regarding user acceptance and user comprehension could be very beneficial.

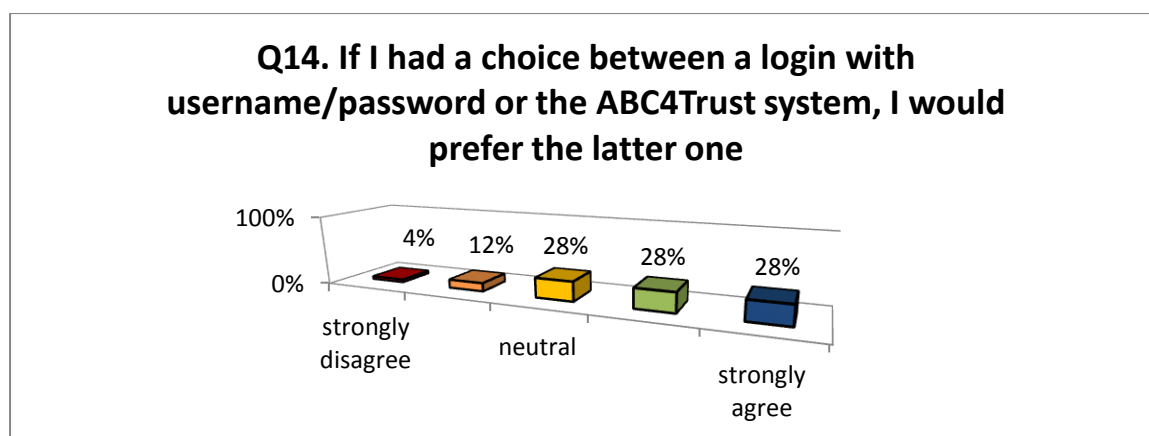


Figure 31: Results of question 14

4.3 Evaluation of User Experience and Feedback: User Acceptance of Privacy-ABC

Understanding why people accept or reject a certain information technology solution is an interesting field of research in the information systems. Investigations started with understanding how the user's beliefs and attitudes on the importance of the provided technology impact the final use. These attitudes and beliefs could also be influenced by other external and less determinant factors.

Different user acceptance models of technology have been proposed in the last decade most of which originate from theories in sociology and psychology. Out of all, the Technology Acceptance Model⁸ (TAM) has a major dominance in the information science society. The TAM was built based on socio-cognitive theory called the Theory of Reasoned Action (TRA). The TRA suggests that a person's behaviour is determined by her intention to perform the behaviour and that this intention is, in turn, a function of his/her attitude toward the behaviour and his/her subjective norm. Intention, often regarded as the best predictor for behaviour, is the cognitive representation of a person's readiness to perform a given behaviour. In this theory, a person's attitude towards behaviour consists of a belief that particular behaviour leads to a certain outcome and an evaluation of the outcome of that behaviour. If the outcome seems beneficial to the individual she may then intend to or even actually do this behaviour.

The TAM as an information systems theory concept based on the TRA tries to model how users come to accept and use a technology. The model suggests that when users are presented with a new technology, a number of factors influence their decision about how and when they will use it. In what follows, we will present the determinant factors affecting technology acceptance privacy ABCs that were incorporated into the final questionnaire distributed to the pupils participating in the Privacy-ABC based Söderhamn school communication system.

4.3.1 Perceived usefulness for privacy protection

The perceived usefulness scale was originally constructed by Davis, Bagozzi and Warshaw with 14 scale items. The authors later revised it and lowered the scale items to 10 items and then to 6

⁸ Proposed by Davis, Fred D., Richard P. Bagozzi, and Paul R. Warshaw. (1989): "User acceptance of computer technology: a comparison of two theoretical models." *Management science* 35.8. 982-1003 (hereinafter referred to as "Davis, Bagozzi and Warshaw").

items. These were further narrowed down to four items. The last four scale items were adapted to evaluate the perceived usefulness of Privacy-ABCs as privacy enhancing tools. The items are used to analyse the extent to which the pilot participants believe that the Privacy-ABC system will be useful in enhancing their privacy during their participation in the Privacy-ABC based school communication for different purposes such as anonymous private chat. After evaluating the questionnaire, we found out that most participants found the system useful for protecting their privacy while using the Restricted Area chat rooms (mean=3.373 σ =1.03 on a 5-point Lickert scale).

4.3.2 Perceived ease of use

The perceived ease of use scale has also gone through similar model maturity as that of perceived ease of use since it was first introduced by Davis, Bagozzi and Warshaw. This concept is defined as the degree to which the technology (information technology system) is regarded as easy to understand and operate without having to exert extra efforts to learn from the user side. The perceived ease of use of the system has an impact on the final technology adoption phase. In addition, it has been noted in technology acceptance research that perceived ease of use has direct and indirect effects towards behavioural intention. The learnability and easiness to use of the Privacy-ABC system was, therefore, analysed by adapting the constructs from the last scales from Davis, Bagozzi and Warshaw. The empirical results show that most participants (m =3.27, σ =1.03 on a 5-points Lickert scale) found the system easy to use.

4.3.3 Perceived anonymity

At the core of ABC4Trust project is the provision of anonymity to the pupils when using the school online communication to exchange information such as online chats, discussion rooms, counselling sessions, and documents sharing. Absolute user anonymity in online services can easily lead to fraud. Whether users should be allowed to stay anonymous online and to what degree of anonymity is even debatable.⁹ Nonetheless, researcher works have been underway to provide anonymity in integration with accountability. Privacy-ABCs, therefore, give a balance of anonymity for honest users and accountability for misbehaving users through a feature called inspection.¹⁰ Whenever a pupil has a problem, be it physical, psychological, mental, financial or any other, they can anonymously discuss it with a counsellor or the school nurse. While pupils can feel assured that their anonymity is well protected, the counsellor can make sure that the user is indeed a pupil of the school and entitled to access the service.

The inclusion of the perceived anonymity concept to our user study allows us to empirically evaluate the sense of anonymity the pupils perceive while communicating in the Restricted Area and other features of the system. The feeling of a sense anonymity helps pupils to be more willing to talk about the real issues they may face, which they would otherwise feel reluctant, shy or scared to talk about if using real identities.

Understanding how anonymity is perceived by the participants, and how they feel about it is a vital issue that affects the final adoption of a privacy enhancing technology such as Privacy-ABC system. We adapted Bosmans and Baumgartner's scales¹¹ to measure the strength of the

⁹ See Kang, R., Brown, S., & Kiesler, S. (2013, April). Why do people seek anonymity on the internet?: informing policy and design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2657-2666). ACM.

¹⁰ See Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., & Rannenber, K. (2012). H2. 1—ABC4Trust Architecture for Developers. *Heartbeat*, 2, 1.

¹¹ See Bosmans, A., & Baumgartner, H. (2005). Goal-Relevant Emotional Information: When Extraneous Affect Leads to Persuasion and When It Does Not. *Journal of Consumer Research*, 32(3), 424-434. (S.426ff.)

psychometric feeling of anonymity of the pupils during Restricted Area chat. The statistical analysis shows that most of the pupils (mean = 3.59, $\sigma = .0966$) strongly felt a sense of anonymity and the feeling that Privacy-ABC system is able to protect their anonymity when they use the Restricted Area.

4.3.4 Privacy-ABCs trustworthiness

Trust, commonly defined as an individual's willingness to depend on another party because of the characteristics of the other party plays an important role in further adoption of technologies.¹² It also plays a central role in helping information technology users overcome perceptions of risk and insecurity by making them comfortably sharing personal information and acting on the system.

In our case, how much the pupils trust the Privacy-ABC system is essentially investigated by incorporating trust measurement psychometric scales adapted from Pavlou's scales.¹³ The analysis shows that majority of the pupils (mean=3.68, $\sigma=0.879$ on a 5-points Lickert scale) believe that the Privacy-ABC system is trustworthy.

4.3.5 Subjective Norm

Subjective Norm (SN) has been defined¹⁴ as an individual's perception of whether people important to the individual think the behaviour should be performed or not. In its purest essence, subjective norm is a kind of peer pressure. Whether or not a person participates or intends to participate in any behaviour is influenced strongly by the people around them. People are also inclined (or not inclined) to participate in a behaviour based upon their desire to comply with others. The contribution of the opinion of any given referent is weighted by the motivation that an individual has to comply with the wishes of that referent. It is a concept that looks at the influence of people in one's social environment on her behavioural intentions.

In our scenario, the beliefs of the pupils, weighted by the importance they attribute to the opinions of the teachers, school principal, parents and peers will influence the behavioural intention to use the Privacy-ABC system. Accordingly, we found out that the pupils are influenced by the people around them to a considerable degree (mean = 3.04, $\sigma = .909$) of accepting the privacy enhanced school communication system.

4.3.6 Behavioural intention to use

The behavioural intention to use is the other psychological construct mainly used to estimate if the users would like to continue using the system. It was first posited in Davis, Bagozzi and Warshaw as a construct mainly affected by the determinant concepts of perceived usefulness and perceived ease of use. Behavioural intention to use also mediates the perceived usefulness and actual system use. As the pupils perceive the Privacy-ABC system to be useful, this consequently influences their behavioural intention to use the system. Furthermore, their perceived ease of use influences perceived usefulness leading to behavioural intention to use and ultimately leading to actual system usage.

We adapted the last scales used in Davis, Bagozzi and Warshaw to measure if the pupils would like to continue the using the Privacy-ABC system if it were to continue in the school. The

¹² See Rousseau, D. M., Sitken, S. B., Burt, R. S. and Camerer, C. (1998). Not so different after all: a cross-discipline view of trust. *Academy of Management Review*, 23, 3, 393-404.

¹³ See Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, 7(3), 101-134.

¹⁴ See Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179-211.

empirical analysis shows that many of the pupils (mean = 3.27, $\sigma = 1.04$) would like to continue using the Privacy-ABC system in the future.

5 Considerations on Legal Topics

5.1 Applicable Law

With the ABC4Trust project being a European one and since project partners from different European countries cooperated in the implementation of the school pilot the question of the applicable national law had to be answered before the start of the pilot. Even after the introduction of a common European data protection framework this question retains its importance since the European Data Protection Directive 95/46/EC is not self-executing but had to be transferred into the national law of the member states. Concerning this transfer the Directive did not only permit a higher standard of protection but explicitly encouraged it.¹⁵ Consequently the different national laws still differ from each other to a certain degree and national particularities have to be taken into account.

Nevertheless, the issue of the applicable law is solved consistently. In regards to the processing of personal data the national law of that EEC member state is applicable in which the controller, who is responsible for the data processing, has established his place of business. Therefore, the applicability is only dependent on where the controller has its headquarter but independent on where in the EEC states the data is processed. This so-called principle of domicile allows controllers to ‘export’ their national data protection laws, when they are processing data in other EEC member states.¹⁶ Therefore, the Swedish Personal Data Act was applicable¹⁷ since the Norrtullskolan was established in Sweden and the data was also collected in Sweden.

Furthermore, the assistance of the Swedish IT company EDOC as well as the Germany based company NSN did not change the applicable law. As the personal data assistant (data processor) is only operating on behalf of the data controller the applicable law and the correlating obligations have to be derived from the controller.

Further and more detailed information regarding the applicable law as well as the contracts between the controller, the data processor and the sub-processor can be found in the deliverable [D53].

5.2 Consent Form and Informing of Users

Simultaneously to the technical setting up of the school communication system the legal foundation of the data processing had to be established. However, neither the Swedish Personal Data Act nor the European Directive 95/46/EC provided a legal permission for the intended data processing but allowed data processing based on the consent of the users.¹⁸ According to Section 3 Personal Data Act a valid consent is

“every kind of voluntary, specific and unambiguous expression of will by which the registered person, after having received information, accepts processing of personal data concerning him or her.”¹⁹

¹⁵ Recital 10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; hereinafter: EU Data Protection Directive 95/46/EC.

¹⁶ Recital 18, Art. 4 (1a) EU Data Protection Directive 95/46/EC.

¹⁷ Section 4 Personal Data Act.

¹⁸ Section 10 Personal Data Act, Art. 7 EU Data Protection Directive 95/46/EC.

¹⁹ Similar Art. 2 (h) Data Protection Directive 95/46/EC

As one can see, a valid consent requires that the user receives information regarding the specific circumstances of the data processing. The Swedish Law, however, does not stipulate the exact scope of which information has to be provided to the user. Nonetheless, while the obligation to inform the user before her consent is distinct from the obligations of informing the registered person in Sections 23 et seq Swedish Personal Data Act they are obviously closely linked.²⁰ In general the goal of the information provided has to be, that the data subject is able to make an informed decision. Therefore, the

*consent by the data subject must be based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, (...).*²¹

Therefore, in a first step the relevant issues of the school pilot had to be clarified. In general the following factors compose the specific circumstances of the processing operation and therefore influence amongst other things the obligation to inform the data subject:

- who will process the data,
- who will be the source of the data,
- for which reasons will the data be collected and processed, and
- which personal data will be processed.

Consequently, a first outline of the pilot set-up showed that it was necessary to inform the users about

- the identity of the data controller, data processor and sub-processor,
- which personal data will be collected and processed,
- for which purpose the data will be processed,
- how the data will be processed (including a high-level and understandable abstract of the automatic means of processing),
- for how long the data will be stored, and
- to whom the data will be disclosed or transferred to.

This information was provided in form of an information sheet which was handed out with the consent form to the possible participants. However, it had to be taken into account, that the users were mostly pupils under the age of 18 years. Thus, the provided information and the consent form had to be understandable for a target group between 13 and 18 years old. Consequently, for the purpose of not overwhelming the reader the information sheet only included the minimum required information. For further information the URL of the ABC4Trust website and the contact details of two contact persons were specified. This information was complemented by a user manual which was given to the participants with their smart cards later on. Furthermore, since it was necessary that the parents or legal guardians of the pupils consented to the data processing as well, it had to be ensured that they received the information too.

Additionally, to ensure the voluntariness of the consent it was stressed in the consent form that no disadvantages would result from not consenting or withdrawing the consent later on.

Nevertheless, after receiving the signed consent forms from the participants the realisation of this

'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

²⁰ Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, Adopted on 13 July 2011, (WP187, 01197/11/EN), p. 19.

²¹ Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, Adopted on 15 February 2007, (WP 131 00323/07/EN), p. 9.

assurance proved to be more problematic than initially thought. Since the number of participants was smaller than initially estimated the situation arose that non-participants and participants were in the same class. Consequently, it was not possible that all communication between pupils and teachers could be done via the school pilot system. Therefore and to safeguard the promise of no disadvantages, the participating teachers were instructed to only communicate non relevant issues via the system or supplement electronic communication with classical means such as letters or phone calls.

Furthermore, for several reasons a paper-based consent form was preferred to a digital one. Firstly, to hand out and collect paper-based consent forms during class or parent-teacher conferences was more convenient than sending out electronic requests. Secondly, an electronic communication before the start of the pilot would have required the collection of the email-addresses of all possible participants. This in itself would have constituted a data-processing which would have presupposed a legal basis. Furthermore, a valid electronic consent would have required that all participants possess a valid digital signature. Finally a paper-based credential was preferred for the sake of proof.

Last but not least, further considerations had to be given from the outset of the pilot to the issue which categories of personal data would be processed. Section 13 Personal Data Act as well as Art. 8 of the Directive 95/46/EC generally forbid the processing of so-called 'sensitive personal data'. This category includes every personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. Exemptions from this prohibition are only permitted in certain scenarios provided by national law or with the consent of the data subject, if the processing of 'sensitive personal data' is explicitly mentioned in the consent form. This prohibition appeared problematical since chat messages of the participants were stored in the system and it could not be predicted what kind of information the participants would disclose in the Restricted Areas of the system. This situation, however, on its own would not have been problematic since the ABC technology would allow users to stay anonymous and would prevent the allocation of chat messages to a certain person. Therefore the information would not have constituted personal data. However, due to legal obligations of the school the inspection feature had to be added to nearly all of the Restricted Areas and participants were only able to interact pseudonymously instead of anonymously. Therefore, their information had to be categorized as personal data. Consequently, to comply with the prohibition of processing sensitive personal data the consent form included a special reference towards the processing of sensitive personal data. Moreover, the inspection feature as well as the inspection grounds were explained in the information sheet. Nonetheless, those Restricted Areas which were most likely to entail political opinions were created as non inspectable and therefore completely anonymous.

5.3 Inspection

One of the more discussed functionalities of the Privacy ABC technology and the school communication system was the inspection feature. By including encrypted additional information into the presentation tokens the users were not able to act anonymously any more. The additional information allowed identifying a user if needed. Therefore, he/she was only interacting pseudonymously. While the widespread inclusion of inspectable Restricted Areas in the communication system prevented that the full capability of the ABC technology was shown it was necessary due to legal obligations of the school. According to Swedish Law the Norrtullskolan is responsible for the safety of the minors. Therefore it was necessary that the school maintained the ability to interfere if the physical and mental safety of a participant would be at risk. Furthermore, since the school provided the communication service to the pupils, they had to assure that the interactions in the system were in compliance with the local anti-discrimination regulations. Nonetheless, the final questionnaire showed that 79% of the users accepted the inclusion of inspectable areas because it gave them a feeling of security to know that someone could help.

In the end it was agreed upon that the Restricted Area, where most likely sensitive personal data was disclosed, stayed un-inspectable. Therefore, the Restricted Area set-up for political discussions was non-inspectable. Nonetheless, it was necessary to set-up counselling sessions as inspectable areas, since pupils might imply a severe threat to their or someone else's life and it would be necessary to identify them.

However, to increase the privacy of the users a strict procedure was agreed upon, and the disclosure of the real identity was only permitted under certain prearranged conditions. These so-called inspection grounds were:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- Breaches of the Norrtullskolan policy against discrimination and degrading treatment.
- An existing court order or other valid administrative request

Furthermore, the inspection feature itself, the technology behind it and the inspection grounds were openly communicated to the participants in the information sheet before they consented to the data processing. Additionally, there were several safeguards in place reminding the participants about the inspection functionality during their interactions in the communication system.

As can be seen in the screenshot below (Figure 32) all the inspectable areas were clearly indicated as such by a small orange 'eye sign'. The 'eye sign' was supposed to explain that someone was watching and could reveal the identity of the user in certain situations. Furthermore, for recognition reasons it was used for other reminders of inspectable areas.

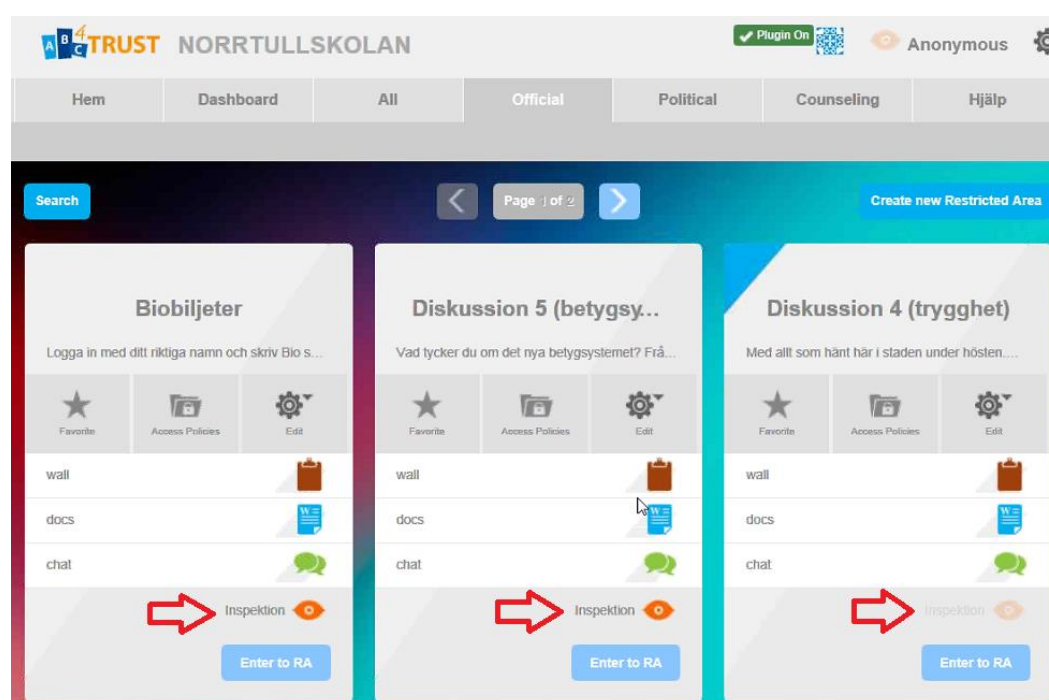


Figure 32: List of inspectable RA indicated with the 'eye sign'

As mentioned before the 'eye sign' was the common indicator in the school communication system for inspectability. Therefore, all the aliases which had been previously used in inspectable Restricted Areas were also marked with it. Thereby, users were supposed to be motivated to create new aliases for different interactions in Restricted Areas, since the more information would be disclosed under the same alias the easier it would get to ascertain the real identity behind an alias. Furthermore, in the case that a pseudonym would have been inspected and revealed all information connected to this pseudonym could have been linked to the real identity of a user.



Figure 33: Inspection indicator - Alias "Superman1000" has been used in an inspectable RA

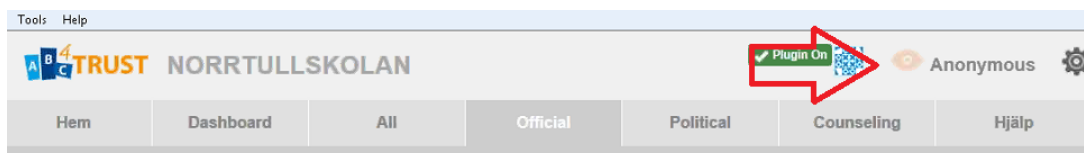


Figure 34: Inspection indicator - Alias "Anonymous" has not been used in an inspectable RA

Last but not least, when requesting a new presentation token in the Identity Selector for an inspectable Restricted Area one was alerted that this token would be inspectable and that the token would include the real identity of the user, even though cryptographically hidden.

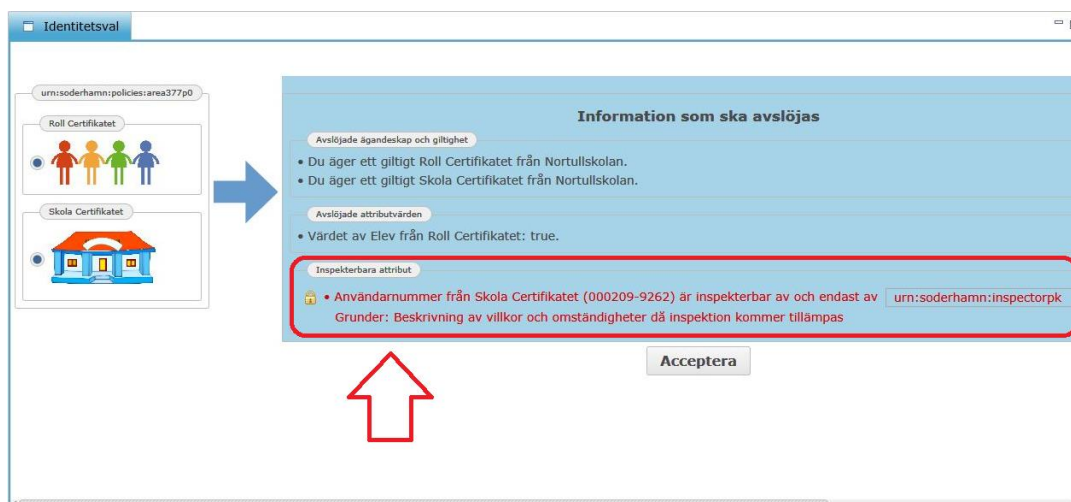


Figure 35: Identity Selector with Inspection warning reminder

However, the final evaluation showed that 35% of the participants were not aware of the fact that they had entered an inspectable area. Therefore, it seems necessary to include even more obvious reminders into a communication system like the one from the school pilot.

5.4 Data Subjects' Rights

Additionally, like in every data processing operation, the issue of data subjects' rights had to be addressed. In Sections 23, 25, 26, 28 of the Swedish Personal Data Act²² the right to be informed, the right of access to data and the right to rectification are stipulated. Nevertheless, in the context of Privacy ABCs the question arises if the processing of data from anonymous or pseudonymous users also demands these users' rights. When responding to this issue one has to differentiate between the data of anonymous and pseudonymous users. Anonymous usage means that there is

²² Similar Art. 10, 12, 14 EU Data Protection Directive 95/46/EC.

no linkage between the identity of the user and the disclosed information like a chat message for example. Hence, completely anonymous data cannot be categorised as personal data and the right of privacy of the user cannot be infringed. Consequently, since data subjects' rights are characteristics of the right to privacy and aim at the effective exercise of one's right to privacy, user's rights are not necessary when anonymous data or data of anonymous users is processed. This result is confirmed by practical considerations since it is literally impossible to provide information about the stored data if requested by a user because it cannot be determined which data is hers. Nonetheless, these considerations cannot be transferred to the data of pseudonymous users. The inspection feature demonstrates that in certain situations the identity of a user can be revealed and therefore, the disclosed data which is linked to her pseudonym can be related to the user. Therefore, whenever there is the possibility, that data can be related to a person, this person has the right to be informed, the right of access to data and the right to rectification.

First of all, the effective exercise of these rights presupposes that a user knows, whom to contact. Therefore, in the information sheet provided before the start of the pilot two persons and their contact details were denominated as responsible contact persons for any requests by the participants.

Furthermore, the right to be informed (Section 23 and 25 Personal Data Act) was complied with by the initial information sheet, the consent form and the user manual handed out with the smart cards. As mentioned above, the information which has to be provided before the consent and the requirements of Section 25 Personal Data Act are not only closely related but overlap mostly. Therefore, no additional information was necessary.

However, more complicated was the implementation of the right of access to data stated in Section 26 Personal Data Act. This right is based on the assumption that the data subject has to know which information is stored about oneself, to effectively exercise his or her right to privacy. Nonetheless, the whole pilot system was designed that users could stay pseudonymously as long as possible and that their real identity would only be revealed in certain extreme situation (inspection grounds). However, the exercise of the right to access would also require the revelation of the real identity of the pseudonymous user to ascertain which information is stored about her. This appears problematic, since inspector and controller/data processor are two different entities and this separation between capacities is necessary to protect users from a possible misuse of personal data. Nevertheless, the data processor/controller is responsible for fulfilling any requests of accessing the stored data. To overcome this problem in the school pilot to some extent the communication system included a feature to check autonomously which information is stored about oneself on the smart card. According to the final questionnaire 26% of the participants used the ABC4Trust browser-plugin tool to inform themselves about their stored data. Moreover, the users were able to read their posted messages in the relevant chat rooms. Consequently, the data subjects themselves had access to the data relating to them.

Furthermore, the participants were informed in the initial information sheets that the whole communication system was a prototype and therefore no strict procedures for requests of rectification, blocking or erasure of personal data were in place during the pilot. Furthermore, due to being a pilot test run the users were not yet able to alter or delete any content or information they had disclosed in the Restricted Areas. Nonetheless, the two above mentioned contact persons were assigned to handle all incoming enquiries and requests on a case by case basis. Moreover, the exercise of the user right to rectification presupposes an unlawful processing of personal data or the processing of incorrect personal data (Section 28 Personal Data Act). Since the processing within the pilot was based on the informed consent of the users the data processing could have only become unlawful if a user would have withdrawn his consent. However, neither this situation arose nor was any incorrect data processed during the pilot and thus, there were no requests for rectification, blocking or erasure of personal data.

5.5 Deletion of Personal Data

Last but not least, the principle of data minimisation demands that personal data is deleted as soon as possible after the purpose of the data processing is accomplished. In accordance with this principle Section 9i) Personal Data Act stipulates that:

The controller of personal data shall ensure that personal data is not kept for a longer period than that as is necessary having regard to the purpose of the processing.

Therefore, the users were informed in the information sheet handed out with the consent forms that their personal data will be deleted the latest six months after the end of the pilot. Therefore, when the users are going to return their smart cards and smart card readers their information stored on the cards will be deleted immediately. Thereafter, and after analysing the stored data of the system and shutting down the communication system, most of the remaining personal data will be erased in the following months. Nevertheless, certain anonymised statistics will be kept for further academic research. Additionally, the consent forms will be kept for six months after the end of the project. Both issues were communicated to the participants in the information sheet and consent form as well.

6 Recommendations and Conclusion

Following the successful implementation and evaluation of the performed two rounds of the school pilot and considering the feedback we received, we suggest the following improvements and recommendations for an even more successful implementation in the future.

6.1 General recommendations

We noted a need to be able to do full-scale testing of a fully integrated system before making decisions concerning parameters and credential specification. The Swedish pilot faced a need for changes after the testing of systems had been done, after integration.

A recommendation for improvement of the School Registration System is to align, from a legal perspective, the idea and implementation in order to allow for the bulk issuance of credentials to improve the process of preparation of cards for pilots.

The conclusion is that the 2nd round of the Söderhamn pilot was overall successful. Issuance, verification, inspection and revocation in combination with the Restricted Area Application functionality served the pilot scenarios well. One important issue that needs to be improved for the future is performance.

6.2 Recommendations for improved performance

The largest efficiency problem (and time consuming with respect to debugging) was by far the smart card. Thus, a recommendation would be to focus on other devices, which fulfill the same purpose with the same security. This could be, e.g. a Smartphone with a tamperproof SIM card or similar device which could do the same computations as the smart card. This means still having to deal with the debugging issues, but it would significantly shorten the development time as the hardware could be supported much better. Also, from a usability point of view, it is much easier to carry around your smartphone as you always do anyway, and just install an app instead of having a smart card and a smart card reader.

Yet another issue a future pilot should take into account is to make the policies used as simple and as few as possible. Each additional condition put into a policy increases the complexity and decreases the efficiency of the system. This also goes for credential specifications, which should be as simple and concise as possible, to lower complexity and strengthen efficiency. Specifically one has to be careful about when to use the power of revocation as this could consume several seconds of each proof due to extra latency because of the revocation authority and added complexity because of the cryptographic layer.

In order to increase efficiency even more, the Verifier could also cache the revocation information needed for the proofs instead of always fetching the latest revocation information. This means that there is a window between the point in time where a credential is revoked and the time the Verifier rejects use of this credential. The tolerated length of this time window would be determined from an analysis of how important it is to prevent bad guys from entering the system.

In general one should cache as much information as possible to save time, but two things in particular are important, namely the PIN code of the user and the values retrieved from the smartcard. The PIN is important to cache as it is in no way a usable system if it continuously asks the user for the PIN code. This means a reduction to security as an adversary could then act as the user if the user leaves the PC without removing her smartcard. Any real system would accept this trade-off though. As for the values from the smartcard, these are important to cache as the communication time with the smart card alone takes up several seconds. Caching data from the

smart card makes sense, as some of the cryptographic evidence might be the same depending on the input to the card.

6.3 Recommendations for Inspection

The Inspection Board has to be defined by the school administration before the system is made available to users, and the Inspection Board needs to be instructed about the usage of the Inspector Application. They also need to develop rules and typical cases for inspection process. An Inspection Board should have representatives from the different groups of users utilizing the system.

From the user side, a recommendation is that whenever inspection functionality is switched on the user should be made aware of this fact in some manner (see Section 5.3).

On the technical side, the Söderhamn pilot built a custom tool called the Inspector Wrapper, a recommendation is to have the User Application extended with Inspector functionality instead. This way a full 'ABCE' based web application could be built using normal ABCE presentation for logging in the Inspector to the application and standard hooks to perform the actual inspection. On top of that, basic functionalities like changing the PIN of the smart card or unlocking the smart card via PUK will then also be inherited. Creating this extension to make the User Application support both normal end user and Inspector functionality is - from WP6 - considered to be a minor task.

6.4 Recommendations for developers

Technical recommendation related to deployment is to agree the usage of common ports for web applications like 443, 8080 and 80 instead of 8443, 8444. This change would decrease the risk of connections being blocked by firewall rules from infrastructure related to the Internet connection used.

Alerts concerning severe errors automatically sent by email from the server to developers, containing technical but not private information, could enhance the bug fixing time. However, such a feature should be implemented with great caution, to make sure not private information can be leaked.

6.5 Recommendations for the Restricted Area Application

The following enhancement suggestions are intended to make the interface of the Restricted Area Application more user-friendly:

The design of the user interface can be improved so that the user is always made aware of switches of aliases (context), by changing the background color of the whole interface or some similar method.

The time it takes to sign in into a Restricted Area should be decreased to the same level as a login using a username and a password.

The addition of a progress indicator to inform the user when the application is busy processing in the background. This would be particularly useful for asynchronous or long operations.

The application should keep track of all attributes exchanged (used or proven) during any communication thread. Which attribute were exchanged, with whom, when did this happen and in which communication thread. This information can be used later to inform the user of how much of his personal data he have revealed and to whom.

The access policy editor GUI used in the pilot to define and add access policies to Restricted Areas was built as a wizard type of user interface. Based on the experience of both rounds of the pilot the conclusion is that a single page layout which shows all possible options on one page would be a more user friendly and faster way of defining access policies. A Mockup of the suggested layout is shown in Figure 36.

Figure 36: Access Policy Editor GUI - a more User friendly Version

6.6 Recommendations from the school administration

Based on the experiences of using Privacy ABC-technologies and the Restricted Area Application during the two rounds of the pilot the school sees many advantages of using a commercial version of the Privacy-ABC technologies to enhance security and to protect the privacy of pupils, teachers and guardian in the future. A commercial solution is expected to be user friendly, fast and should offer functionalities that are needed by a modern school.

For the pilot to operate properly, the school had to change some firewall settings of the school network to allocate some communication ports needed by the school pilot system. As a recommendation for the future a new application such as the Restricted Area Application based on Privacy-ABC technologies should work properly without the need of changing the firewall settings of the school. Therefore, it would be a good idea to use standard communication ports.

One issue that was discussed at the school was if the RA Application would imply or add more workload on the school personnel. The school's main goal and priority is on educating the pupils, and all applications used should support this main goal without adding more workload. In order to avoid adding more workload on school personnel or the need of using several different systems a recommendation from the school is that a new system needs to have more functionality that are needed by a school.

Implementing a new system within the school domains should, whenever possible, be integrated into the existing systems already used by the school. A recommendation is that a future version of the IdM (Issuer) should retrieve data automatically from the schools own administrative systems, where all the personal data about the users already exists. In that way changes have to be done only in one system.

6.7 Conclusion

This pilot successfully offered a privacy-respecting social platform, Restricted Areas, to the pupils so that they could have a flexible means of not only communicating with each other, but with key adults who had an interest in their education and lives. By utilizing the Privacy-ABC technologies, the users of the Söderhamn pilot remained in full control of what level of personal information they disclosed, if any at all, to whomever and whenever. In hindsight, we can see that the users were able to utilize the Restricted Area Application in the way it was intended to be used with teachers creating Restricted Areas and defining access policies while the pupils and their guardians could enter defined Restricted Areas and post and receive messages and documents, etc.

Overall the users had a good level of understanding and appreciated the overall concept of the Privacy-ABC technology. As part of the pilot's success evaluation, at the end of the pilot duration we incorporated methodological survey questions to determine how the pupils react to the importance of the Privacy-ABC system in enhancing their privacy. A well-established model called the Technology Acceptance Model (TAM) was used as a basis to build the questionnaire concepts. The overall statistical analysis demonstrates that the pupils understood and trusted the system and that it improves their privacy when performing different activities such as anonymous chatting with other peers, parents or school teachers. Other measurement concepts also showed that many pupils would use the system if it were to continue operating.

The technological considerations were many, however all of the process in place allowed for a relatively smooth implementation, deployment and operation within all the areas we had intended to address. This does not mean that there were not any bumps in the road along the way, but that the processes in place for isolation and debugging allowed for quick turnaround for solutions. The Söderhamn Pilot rigorously and successfully tested and improved the technologies to an overall solid system. A successful commercial version of these technologies in the future would require enhancements to be made with regard to the overall performance.

While these technologies were successful within the contained scenarios of the test pilots, how these privacy-preserving tools can be implemented in a more multifaceted situation may not be as straightforward. Assuming the implementation of this technology will be complex and specific to each installation, the solution will likewise be unique and without specific directions. Additionally it will require service providers to rethink the way they give access and identify their customers, while the users need to be informed about what personal information they are sharing and whether inspection is on or off for a particular service/section.

Appendix A User's Questionnaires

The following documents are included in the pages that follow.

A.1 User's Questionnaire – First round – English version

A.2 User's Questionnaire – First round – Swedish version

A.3 User's questionnaire – Second round – English version

A.1 User's Questionnaire - First round - English version

The Pupils participating in the first round were presented with a set of tasks to test, and a questionnaire related to the tasks.

The tasks were

- A. Try to log in to a list of Restricted Areas.
- B. Create a Restricted Area and post a message to it.
- C. Use a Restricted Area for around 2 minutes, while other users also use the same Restricted Area.

The questionnaire contains a first part asking which of the Restricted Areas in task A the user could log in to, a second part asking if the user performed tasks B and C, and a part with the following questions on general user satisfaction:

10. Do you like the idea of this technology?
11. Do you think you understood the menus and how to use the system?
12. Did you find the response times acceptable?
13. Do you think you would use the system in the future?

These were followed by two open questions:

14. What did you like (about the system)?
15. What did you dislike (about the system)?

A.2 User's Questionnaire - First round - Swedish version

ABC4Trust

Hej, vi har skapat några uppgifter som vi vill be er att utföra i syfte testa systemet. Alla som deltar kommer att få två biobiljetter var. De som lyckas skapa en egen Restricted Area och kan logga in på den och skicka ett meddelande kommer att få en extra biobiljet. Och de som deltar överbelastningstestet kommer att få ytterligare en biobiljett. Totalt har man chansen att få 4 biobiljetter om man utför följande:

- A. Logga in på de Restricted Areas som finns i formuläret och fyll svara på formuläret. (2 biljetter)
- B. Skapa en Restricted Area och logga in på den och skicka ett meddelande (1 biljett)
- C. Samtidig inloggning (ca 2 minuter) för att testa systemets överbelastningskapacitet (1 biljett)

Deluppgift A. Logga in på de 7 olika Restricted Areas som finns i frågeformuläret (Deluppgift A.)

1. Surfa till startsidan www.abc4trust.se och klicka på "Gå till applikationen" under "Restricted Area"
2. Ange din PIN-kod och bekräfta
3. Välj ditt riktiga namn som alias när du loggar in.
4. Klicka på "Alla RA" i huvudmenyn.
5. Utför (punkterna a, b, c och d) för var och en av de Restricted Areas som finns listade i frågeformuläret. Fyll i formuläret om du lyckades eller inte.
 - a. Försökt att logga in på de Restricted Areas som finns i frågeformuläret
 - b. Skicka ett meddelande i chatten som t.ex. "Hej, ..."
 - c. Klicka på "Väggen" och skriv (skicka ett meddelande) på väggen t.ex. "Hej, ..."
 - d. Prova gärna att ladda upp ett dokument/en fil (PDF eller MS-Word format eller annat)

Obs. Man ska inte kunna logga in på alla RA. (t.ex. elever från årskurs 7 kan inte logga in på en RA för årskurs 8 osv.)

Deluppgift B. Skapa en Restricted Area

1. Välj "Mitt skrivbord" i huvudmenyn
2. Klicka på knappen "Skapa en ny Restricted Area" (längst upp till höger)
3. Ange ditt namn som namn på RA. Klicka på "Spara och gå vidare" och följ instruktionerna tills du har skapat en RA.
4. Nu ska du under fliken "Policy" klicka på "+" och acceptera "Policy 1" som namn.
5. Klicka på det nya "+" som dyker upp ovanför "Attribut (egenskaper)"
6. Nu ska du lägga till två villkor
 - a. "First Name" = Nisse (Byt Nisse mot ditt eget förnamn)
 - b. "Last Name" = Svensson (Byt Svensson mot ditt eget efternamn)
7. Försök att logga in på den RA som du skapat och skicka meddelandet "Jag lyckades ..."

Deluppgift C. Samtidig inloggning på Restricted Area som heter "Belastningstest". Tid meddelas senare

1. Välj "Alla RA" i menyn och klicka på Restricted Area som heter "Belastningstest"
2. Logga och börja testa att använda det under ca 2 minuter, mellan kl. 20:00-20:02
 - a. Skicka några meddelanden under Chatten
 - b. Skriv något på Väggen
 - c. Ladda upp och ladda ner några dokument under fliken "Dokument"
3. Det är viktigt att man är inloggad och använder systemet under dessa 2 minuter

Frågeformulär

Deluppgift A. Vänligen ange om du kunde logga in eller inte på dessa Restricted Areas.

#	Restricted Area Namn	Lyckades logga in	Lyckades inte logga in	Försökte inte	Kommentarer
1	Alla	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2	Flickor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	Pojkar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4	Årskurs 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5	Årskurs 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6	Årskurs 9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7	Frågor och svar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Deluppgift B & C

#	Fråga	Ja	Nej	Ej svar	Kommentar
8	Har du utfört deluppgift B?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9	Har du utfört deluppgift C?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Frågor om tekniken och systemet i allmänhet

#	Frågor	Ja	Nej	Vet ej	Kommentar
10	Tycker du att idén bakom tekniken verkar bra?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
11	Tycker du att man förstår menyerna och hur systemet ska användas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12	Tycker du att svarstiderna är acceptabla?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
13	Tror du att du skulle använda systemet i framtiden?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Dina övriga kommentarer och synpunkter om projektet, systemet och tekniken.

14	Vad tycker du är bra?	
15	Vad tycker du är dåligt?	

A.3 User's questionnaire - Second round - English version



Survey at Söderhamn School, Sweden

Thank you for participating in our survey!

Your support provides an important contribution to the success of the ABC4Trust project.

When you answer the questions, your own opinion is important, hence there are **no right or wrong answers** to the questions. You are kindly requested to answer the questions consciously and completely.

Please note that some of the questions may seem repetitive to you, but they are made so for more accurate measurements.

All information gathered will be used for improving the Privacy-ABC system and correlating academic purposes ensuring that no one will be able to know your identity based on the answers provided.

Souheil "Sosso" Bcheri
Managing director, Eurodocs

Mobile: +46 (0)70 602 42 42

Fax: +46 (0)270 766 05

E-mail: sosso@eurodocs.net

Homepage: www.eurodocs.net

Questionnaire - Part 1

No Yes

Q1. Have you ever used more than one alias? O

(Other than the standard one provided to you at the beginning of the pilot with your real name)

Q2. If yes, were you nevertheless aware which one you were using all the time? O

Q3. Please look at the screenshot below. If you would want to login and access this Restricted Area and click on the bottom “Accept”, which of the following information about your self are you proving and revealing to the system?



- Your name
- Your age
- That you are older than 13 years
- Your class
- That you are a pupil **(The correct answer)**

Q4. Have you used the ABC4Trust browser-plugin tool to check which data is stored about you on your smart card?

No Yes

O O



Q5. Please look at the screenshot below showing the access policy of a certain Restricted Area. What do you think which of the following persons or group of persons would be allowed to enter this restricted area? Please select:

Access Policies		
Alias Policy		
Attributes	Funktion	Värde
Alias Name	=	Snyggast
Policy 1		
Attributes	Funktion	Värde
Kön	=	female
Ålder	>=	13

- All girls
- All persons older than 13 year
- All pupils
- All girls 13 years or older (The correct answer)
- All female teachers



Q6. Have you ever been in an inspectable area within the ABC4Trust system? No Yes

Q7. And were you aware of this fact?

Q8. **If yes**, did this give you a feeling of security because you knew that someone could help if anything would go wrong?

Q9. Have you ever entered a chat room which had limited access for a certain group of pupils (e.g. only girls/ only boys)?

Q10. **If yes**, were you confident that all other members in this chat were allowed to be there?

Q11. Have you ever created a restricted area with limited access for a certain group?

Q12. Did you ever try to sneak into a Restricted Area with limited access for a certain group to which you should not have access to?

Q13. **If yes**, did you succeed?

Q14. If I had the choice between a login with username/password or the ABC4Trust system, I would prefer the latter one.

	Strongly		Strongly	
	Disagree			agree
	1	2	3	4
	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
			5	
			<input type="radio"/>	

Questionnaire - Part 2



Q15. Please indicate how strongly you agree or disagree with the following statements. The questions focus on how **useful** and **easy** you found the ABC4Trust portal system.

	1	2	3	4	5
Using the ABC4Trust portal improves my privacy protection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I find the ABC4Trust portal to be useful in protecting my privacy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using the ABC4Trust portal increases my privacy protection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My interaction with the ABC4Trust portal is clear and understandable.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interacting with the ABC4Trust portal doesn't require a lot of my mental effort.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I find the ABC4Trust portal to be easy to use.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I find it easy to get the ABC4Trust portal to do what I want to do.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

⌏ Please turn ₂



Q16. Please indicate how strongly you disagree or agree with the following statements. The questions focus on how you would **intend to continue using the ABC4Trust portal** if it were to continue. Some of the questions concern as to how **others influence you** to use the system.

	Strongly disagree				Strongly agree
	1	2	3	4	5
Assuming that the ABC4Trust portal is available, I intend to use it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Given that the ABC4Trust portal is available, I predict that I would use it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would use the ABC4Trust portal in the next year.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My teachers think that I should use the ABC4Trust portal.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other pupils think that I should use the ABC4Trust portal.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The principal of my school thinks that I should use the ABC4Trust portal.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7 Please turn 3



Q17. Please indicate how strongly you agree or disagree with the following statements. The questions focus on how **trustworthy** and **anonymity protecting** you found the ABC4Trust portal system.

	Strongly disagree		Strongly agree		
	1	2	3	4	5
The ABC4Trust portal system is trustworthy.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The ABC4Trust portal system is one that keeps promises by not disclosing more information than needed.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I trust this ABC4Trust portal system because it notifies me what personal information I'm disclosing.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The ABC4Trust portal is able to protect my anonymity when I use the Restricted Area.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
With the ABC4Trust portal I obtain a sense of anonymity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The ABC4Trust portal can prevent threat to my anonymity during Restricted Area chat on the system.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Finally, we have some questions regarding your personal information. All data will be treated strictly anonymous and only used for the project's academic purposes.

Q18. Age:	12, 13, 14, 15, 16, 17, 18+		
Q19. Gender:	<input type="radio"/> Female	<input type="radio"/> Male	
Q20. Role:	<input type="radio"/> Pupil	<input type="radio"/> Guardian	<input type="radio"/> Teacher

Thank you for your time and participation!

Appendix B Legal Forms

The following is included in the pages that follow.

The English version of the documents:

- B.1 Information sheet for pupils/participants and parents/legal guardians - English version
- B.2 Consent form for pupils/participants and parents/legal guardians - English version
- B.3 Information sheet for school staff – English version
- B.4 Consent form for school staff – English version
- B.5 Legal Notice and privacy policy of the website – English version

B.1 Information sheet for pupils/participants and parents/legal guardians - English version



Consortium of the EU/FP7 programme-funded Research project ABC4Trust

Norrtullskolan and Eurodocs

Information sheet for the Söderhamn pilot participation in the research & development project ABC4Trust

Dear pupil/participant, dear parent/legal guardian,

The consortium of the European Commission-funded research and development project ABC4Trust would like to invite the pupils of all classes in the 7th-9th grade of the Norrtullskolan in Söderhamn, Sweden to participate in a trial to test the deployment of a so-called Privacy-ABC technology system.

In the following, this fairly new technology designed to protect the identity and the privacy of pupils engaging in digital communication within a dedicated online platform of our school will be explained.

Let us introduce to you some of the capacities of this technology and the goal of the ABC4Trust project, especially with regard to the Söderhamn school pilot.

What is it all about? And what are Privacy-ABCs?

The abbreviation “Privacy-ABC” stands for “Privacy enhancing Attribute-based Credentials”. Privacy-ABCs enable individuals preserving their privacy whenever they need to identify or register for an Information and Communication Technology (ICT) system in the digital sphere such as the internet. This may be for example the registration on a website for online-shopping, for a discussion forum, in a social network, or for anonymous polling and voting.

While surfing the web, often a full-disclosing secure authentication or identification is required (you may know this from Facebook or similar networks), leaving the person only with the option to reveal their own identity to be able using the offered service. Moreover, in most cases service providers demand a whole lot more information than absolutely necessary to provide their service. But these demands severely threaten the privacy of the users!

Privacy-ABCs allow the user to only reveal the information absolutely necessary for the execution of the required action, and thus respect the privacy of the individual!

How does this work? Only a set of so-called “credentials” and not all information of the user are provided to the system. In this context, “credential” means only a single bit of information that is necessary for the user’s eligibility of using a specific digital service (such as a certain forum or chat room). Those “credentials” can be the proof that the

owner of the credential is indeed pupil of a particular school, of a particular class, or of a specific age. This information can be verified by the digital credential without revealing other, unrelated and unnecessary information about the user.

For example, a certain service may require that a person is of a certain age or older before it can be used. By using credentials, it is possible verify a certain age (e.g. older than 14 years) without giving away the exact birthdate. Thus, Privacy ABCs enable a **minimal disclosure of personal data** of the user, making an anonymous and pseudonymous usage of most different IT services possible.

What is the ABC4Trust project?

ABC4Trust is a research and development project funded by the European Commission under its 7th Research Framework Program (FP7) as part of the ICT Trust & Security programme. The project name is an acronym which stands for “Attribute-based Credentials for Trust”. The ABC4Trust project has gathered partners from different countries of Europe. The Söderhamn Kommun is one partner of the project and is presenting the project pilot launch at the Norrtullskolan.

Having started in November 2010 with duration of four years, the project aims at achieving a more thorough understanding of Privacy-ABC’s by enabling the deployment in practice and their federation in different domains. In doing so, the project team runs pilots, also called trials, in various environments. This is done to obtain real user feedback on Privacy ABC systems and to learn how good the so far developed system works. Hopefully, these trials will give the opportunity to test the use and performance of the technology with the help of users with different skills and needs. For more information about ABC4Trust, please visit our website at www.abc4trust.eu.

The Söderhamn pilot

The ABC4Trust project launches a pilot deploying Privacy-ABC’s at the elementary school Norrtullskolan in Söderhamn, Sweden. This pilot will integrate several types of digital communication between pupils, guardians and school personnel needed by the school. Today, Swedish schools mainly use the public Internet as the means of school-related communication. However, using correlating public IT-services currently available in the web severely lack proper protection of the pupil’s and their guardian’s privacy. This especially occurs if the same username is used in different settings, allowing cross-context linkage and revelation of identity. But Swedish schools are also obliged by laws and regulations to inform the guardians when a pupil is absent from a class. In addition, schools are obliged to create individual teaching plans for each student. Such 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-ABCs to enable secure and by minimal data disclosure, privacy-preserving identification in communications between staff, pupils and guardians. The first pilot application at the Norrtullskolan will involve privacy-preserving community access and school internal social networking for pupils via a specifically dedicated online platform. Thereby, this pilot addresses the specific challenges posed by the fact that internet users get ever younger and often are minors.

The communication services provided on the online platform entail the following possibilities for the participants:

- Chat rooms to be used by pupils and/or staff
- Online forums for discussing lessons and other school related matters as well as political discussions. These may be set up as openly accessible forums or as personal Restricted Areas where only a predefined group of participants can enter (e. g. children of a certain age or class).
- Online counselling sessions in Restricted Areas with health personnel (counsellors, social workers, nurses, coaches), where staff can provide counselling in a safe environment while pupils are not necessarily required to reveal their identity.
- Document areas where staff can share documents (e.g. grades and development plans) with pupils and their guardians.
- Online polls set up by the school staff

Especially in the context of counselling, when not being forced to reveal their identity, pupils may be more willing to talk about the real issues they may face which they would otherwise feel reluctant, shy or scared to talk about. However, to guarantee the physical and mental safety of each participating pupil, the ABC system foresees in those Restricted Areas Restricted Areas for counselling the revelation of the pupil's identity (called inspection) in certain predefined emergency situations (called inspection grounds). Such inspection grounds can be:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- Situations demanding an intervention according to the Norrtullskolan policy against discrimination and degrading treatment. This policy can be found at <http://bit.ly/1e7ptSm> for further reading.
- An existing court order or other administrative request binding for Norrtullskolan or Söderhamn Kommun

In case a participant (pupil, legal guardian, or school staff) reports an emergency situation, it will in a first step always be investigated by an assigned School Inspection Board. This Board will evaluate the claimed reason for the inspection, and in case it is valid, it triggers a formal inspection process, forwarding the request to an assigned Inspector. This Inspector will perform a double check and is equipped with the technical capability to reveal the identity of the pupil. The whole process will also be protocolled. This procedure guarantees that no single entity is able to arbitrarily spoil the privacy of the pupil and the identity is revealed in emergency cases only. If the School Inspection Board decides that the case does not require the identification of the user, it either closes the case or may decide to delete the content and/or write a warning to the respective Restricted Area.

Besides the inspection procedure described above other possibilities to track the user's behaviour such as storing IP-addresses or setting cookies are not strictly necessary in the system used for the Restricted Areas. However, for usability reasons and to avoid the necessity to frequently re-authenticate with the smartcard, session cookies are used but each change of alias names creates a new session with different cookies preventing

tracking across sessions. The separate system for issuing the necessary credentials for later use on the Restricted Area system requires session cookies for its operation, but there the user is identified by name anyway. Beyond this the sites abc4trust.se and portal.abc4trust.se do not use cookies unless the language selector is set to another language as Swedish. Here a cookie is used to set the preferred language.

Who is involved in the trial?

- Teachers and other school personnel (also called staff)
- Pupils of grades 7, 8, 9 (all – A,B,C,D), excluding ones whose parents refused their children to participate in the pilot
- Guardians of pupils who participate

The total quantity of users in this pilot is more than 800 people. The participation in the trial is **free and voluntary**. In case the pupil of the class targeted for the trial wishes to participate, he/she can ask questions at any point in time by directing the enquiries to a contact person which is named below.

How does the pupil participate in the pilot?

For the duration of the trial, the pupil will receive a set of credentials which will be stored on a smart card provided by the school. The pupil will receive the credential smart card together with an appropriate card reader to connect with the pupil's own personal computer at home or with a PC at the school. The credentials on the smart card are protected by a PIN known only to the participant. Thus, the pupil will receive the following requisites for the pilot:

- Smart card
- One-time password for the smart card (PIN)
- Card Reader

With the credentials stored on the smart card, pupils will be able to identify themselves for access to restricted chat rooms and restricted information in the IT system provided for the school. Thereby, they will be able to remain anonymous when asking private and sensitive questions from school personnel. But also, the school personnel can ensure that it communicates with the right 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 to use a many-step procedure to enter a school site. Whenever the pupil wants to access a certain IT service provided for the school (as mentioned above), the integrated ABC system provides an online interface between the browser and her smart card. For this reason, it employs a software component called "User Client" that runs locally on the pupil's PC. This software component is triggered every time a participant is required to provide data stored on her card and asks for consent. Moreover, it enables the pupil to browse, delete, or locally backup the Privacy-ABCs stored on the own smart card. A number of card readers will also be available in the school, connected to common computers. For more in-depth explanation and help regarding the handling of the smart card, the User Client software, how to obtain credentials or to participate in

school internal IT services, please refer to the pilot handbook available at the pilot's portal page: www.abc4trust.se

What happens with the personal data?

For the usage of the school internal IT services as described above, the following personal information from the participants will be used within the pilot:

- First name
- Last name
- School
- Class
- Gender
- Date of birth
- Subject (meaning individual school courses, such as maths, English, physics etc.)

The named data is securely stored in a School Registration System which is run and administered by the ABC4Trust project partner Eurodocs. The processing is necessary for the purpose of issuing respective credentials to be stored locally on the smart cards of the participants and to re-issue credentials in case of lost cards. In addition, access to this data may become necessary for Eurodocs to ensure and measure the functionality of the pilot system and for tracking and remove errors.

Participants have the possibility to access and rectify data stored in the School Registration System online, or by contacting Eurodocs or the school. Eurodocs is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN), Munich, Germany, in setting up, running, and administering the School Registration System. For this it may become necessary to grant employees of NSN physical or online access to the School Registration System for administration purposes, validation of the system's functions as well as tracking and removing of errors.

To protect the participant's personal data, precautions have been made. NSN can only access the system under the supervision of Eurodocs. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by Eurodocs employees or online. In this case, the personal data underlies the same security requirements as if it would reside with the school. Any communication between NSN and the School Registration System will be protected against unauthorized access by third parties. Retrieved credentials are stored on the smart card under the control of the participant and accessible only with the PIN which will be handed out to the participants.

All personal information provided by the participating pupils will be treated carefully and confidentially. It will be stored securely and will not be used or disclosed to third parties without the pupil's and their parent's explicit consent.

Since this pilot is part of scientific research project, aggregated and anonymised data will be used to complete the research work of this project as well as it will be used for academic purposes, like the publication of scientific proceedings; for drafting various informative reports, containing presentations of graphs and statistics that will be publicly available. The personal data in the collected, stored and processed will be deleted 6 months after the end of the trial.

User consent and effect of not consenting

The processing of personal data in this pilot falls under the scope of the Swedish protection law. To lawfully process this data, the school needs an informed consent of each participant. A consent form is attached to this information sheet.

The pupils and their responsible parents/legal guardians are free to give consent and an already provided consent may be revoked any time by notice towards the school. Not providing consent or revoking it later will not cause any disadvantages in class. Please note that without giving consent, the pupil may not participate in the trial.

Contact details of the responsible parties for questions and other inquiries:

Norrtullskolan, Norrtullsgatan 13, Söderhamn, Goran.Hanell@soderhamn.se, 0270-75759

Eurodocs AB, S:a Hamngatan 50, 826 50 Söderhamn, sosso@eurodocs.net, 070-5 742 742

More information about the project can be found at: www.abc4trust.eu

More information about the ABC system can be found in the user manual at: www.abc4trust.se/portal/help/usermanual

Come and join our school pilot – we'd be happy to welcome you and your participation in the ABC4Trust pilot trial!

Sincerely yours,

Norrtullskolan and Eurodocs

B.2 Consent form for pupils/participants and parents/legal guardians - English version



Consortium of the EU/FP7 programme-funded Research project ABC4Trust
Norrtullskolan and Eurodocs

Consent form for the ABC4Trust Söderhamn pilot participation

This consent form addresses you as a participant and/or responsible parent/legal guardian in the first trial of a Privacy-ABC system at the Norrtullskolan within the EU-funded research and development project ABC4Trust. During this trial, the participant's personal data as stated above will be collected, stored and processed by the Eurodocs. Self provided user content may also concern sensitive personal data. For this, Norrtullskolan kindly asks you for your written consent to process the said personal data. For an explanation of the system deploying Privacy-ABCs that will be tested and the type of personal data processed for which purposes, please refer to the information sheet handed out as attachment to this form. Further information about the technical specifics can be found under the project website (www.abc4trust.eu), and especially in the user manual that is provided online at: www.abc4trust.se/portal/help/usermanual.pdf

Inter alia, this personal information will be processed during the trial:

- First name
- Last name
- School
- Class
- Gender
- Date of birth
- Subject (e. g. maths, English, physics etc.)

Beyond these bits of personal data used to enable the creation of the credentials and correlating accesses to the system, other personal data may find its way into the system through the content uploaded by the participants themselves, e.g. in the forums. While using the system participants may reveal particularly sensitive information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life.

Eurodocs is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN), Munich, Germany, in setting up, running, and administering the School Registration System (data processor). For this it may become necessary to grant employees of NSN physical or online access to the School Registration System for administration purposes, validation of the system's functions as well as tracking and removing of errors. To protect the participant's personal data, precautions

have been made. NSN can only access the system under the supervision of Eurodocs. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by Eurodocs employees or online. In this case, the personal data underlies the same security requirements as if they would reside with the school. Any communication between NSN and the School Registration System will be protected against unauthorized access by third parties. In accordance with the principles of the Swedish Personuppgiftslagen (PUL) (<http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/>), all personal information provided by the participating pupil and related parents will be stored securely and will not be used or disclosed to third parties without explicit consent to do so. The participation in this trial will be completely confidential and personal data will be averaged and reported in aggregate. The personal information provided while using the above described services will only be used for the completion of this research project; in aggregated (i. e. anonymised) form for academic purposes, like the publication of scientific proceedings; for drafting various informative reports, containing presentations of graphs and statistics that will be publicly available. If any questions about these procedures remain, please refer to the responsible person at Norrtullskolan, Göran Hånell for any further inquiry or explanation. If the participating pupil does not wish to complete this trial, we kindly ask to inform Göran Hånell and he/she will facilitate the withdrawal from the trial. Not consenting or revoking consent does not have negative implications on a participation in class. This consent form will be securely kept with Norrtullskolan until 6 months after the end of the project.

Please express your consent regarding the above described trial participation below:

- By signing this consent form below, I indicate that I have read and understood the terms and conditions of the trial.
- **As parent/legal guardian**, I hereby explicitly consent that my child may voluntarily take part in the trial.
- **As pupil**, I hereby consent to participate in the trial under the above described terms.

The explicit expression of consent includes the later usage of the collected and processed personal data in aggregated (i. e. anonymised) form for scientific research aimed at improving the Privacy-ABC technology and for correlating research and dissemination publications.

Date :

Name of participating pupil :

Class of participating pupil :

Signature of participating pupil :

Name of at least one responsible legal guardian :

Signature of at least one responsible legal guardian :

Please give the signed consent form to: Göran Hånell

Contact information: Norrtullskolan, Norrtullsgatan 13, Söderhamn,

Goran.Hanell@soderhamn.se, 0270-75759

B.3 Information sheet for school staff - English version



Consortium of the EU/FP7 programme-funded Research project ABC4Trust
Norr tullskolan and Eurodocs

Information sheet for the Söderhamn pilot participation in the research & development project ABC4Trust

Dear member of school staff,

The consortium of the European Commission-funded research and development project ABC4Trust would like to invite the teachers of all classes in the 7th-9th grade of the Norrtullskolan in Söderhamn, Sweden to participate in a trial to test the deployment of a so-called Privacy-ABC technology system. Moreover, other school staff responsible for the chosen set of classes, e.g. counsellors, social workers, nurses, coaches etc., are invited to participate in this trial.

In the following, this fairly new technology designed to protect the identity and the privacy of pupils engaging in digital communication within a dedicated online platform of our school will be explained.

Let us introduce to you some of the capacities of this technology and the goal of the ABC4Trust project, especially with regard to the Söderhamn school pilot.

What is it all about? And what are Privacy-ABCs?

The abbreviation “Privacy-ABC” stands for “Privacy enhancing Attribute-based Credentials”. Privacy-ABCs enable individuals preserving their privacy whenever they need to identify or register for an Information and Communication Technology (ICT) system in the digital sphere such as the internet. This may be for example the registration on a website for online-shopping, for a discussion forum, in a social network, or for anonymous polling and voting.

While surfing the web, often a full-disclosing secure authentication or identification is required (you may know this from Facebook or similar networks), leaving the person only with the option to reveal their own identity to be able using the offered service. Moreover, in most cases service providers demand a whole lot more information than absolutely necessary to provide their service. But these demands severely threaten the privacy of the users!

Privacy-ABCs allow the user to only reveal the information absolutely necessary for the execution of the required action, and thus respect the privacy of the individual!

How does this work? Only a set of so-called “credentials” and not all information of the user are provided to the system. In this context, “credential” means only a single bit of information that is necessary for the user’s eligibility of using a specific digital service (such as a certain forum or chat room). Those “credentials” can be the proof that the owner of the credential is indeed pupil of a particular school, of a particular class, or of a specific age. This information can be verified by the digital credential without revealing other, unrelated and unnecessary information about the user.

For example, a certain service may require that a person is of a certain age or older before it can be used. By using credentials, it is possible to verify a certain age (e.g. older than 14 years) without giving away the exact birthdate. Thus, Privacy ABCs enable a **minimal disclosure of personal data** of the user, making an anonymous and pseudonymous usage of most different IT services possible.

What is the ABC4Trust project?

ABC4Trust is a research and development project funded by the European Commission under its 7th Research Framework Program (FP7) as part of the ICT Trust & Security programme. The project name is an acronym which stands for “Attribute-based Credentials for Trust”. The ABC4Trust project has gathered partners from different countries of Europe. The Söderhamn Kommun is one partner of the project and is presenting the project pilot launch at the Norrtullskolan.

Having started in November 2010 with duration of four years, the project aims at achieving a more thorough understanding of Privacy-ABC’s by enabling the deployment in practice and their federation in different domains. In doing so, the project team runs pilots, also called trials, in various environments. This is done to obtain real user feedback on Privacy ABC systems and to learn how good the so far developed system works. Hopefully, these trials will give the opportunity to test the use and performance of the technology with the help of users with different skills and needs. For more information about ABC4Trust, please visit our website at www.abc4trust.eu.

The Söderhamn pilot

The ABC4Trust project launches a pilot deploying Privacy-ABC’s at the elementary school Norrtullskolan in Söderhamn, Sweden. This pilot will integrate several types of digital communication between pupils, guardians and school personnel needed by the school. Today, Swedish schools mainly use the public Internet as the means of school-related communication. However, using correlating public IT-services currently available in the web severely lack proper protection of the pupil’s and their guardian’s privacy. This especially occurs if the same username is used in different settings, allowing cross-context linkage and revelation of identity. But Swedish schools are also obliged by laws and regulations to inform the guardians when a pupil is absent from a class. In addition, schools are obliged to create individual teaching plans for each student. Such 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-ABCs to enable secure and by minimal data disclosure, privacy-preserving identification in communications between staff, pupils and guardians. The first pilot application at the Norrtullskolan will involve privacy-preserving community access and school internal social networking for pupils via a specifically

dedicated online platform. Thereby, this pilot addresses the specific challenges posed by the fact that internet users get ever younger and often are minors.

The communication services provided on the online platform entail the following possibilities for the participants:

- Chat rooms to be used by pupils and/or staff
- Online forums for discussing lessons and other school related matters as well as political discussions. These may be set up as openly accessible forums or as personal Restricted Areas where only a predefined group of participants can enter (e. g. children of a certain age or class).
- Online counselling sessions in Restricted Areas with health personnel (counsellors, social workers, nurses, coaches), where staff can provide counselling in a safe environment while pupils are not necessarily required to reveal their identity.
- Document areas where staff can share documents (e.g. grades and development plans) with pupils and their guardians.
- Online polls set up by the school staff

Especially in the context of counselling, when not being forced to reveal their identity, pupils may be more willing to talk about the real issues they may face which they would otherwise feel reluctant, shy or scared to talk about. However, to guarantee the physical and mental safety of each participating pupil, the ABC system foresees in those Restricted Areas for counselling the revelation of the pupil's identity (called inspection) in certain predefined emergency situations (called inspection grounds). Such inspection grounds can be:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- Situations demanding an intervention according to the Norrtullskolan policy against discrimination and degrading treatment. This policy can be found at <http://bit.ly/1e7ptSm> for further reading.
- An existing court order or other valid administrative request

In case a participant (pupil, legal guardian, or school staff) reports an emergency situation, it will in a first step always be investigated by an assigned School Inspection Board. This Board will evaluate the claimed reason for the inspection, and in case it is valid, it triggers a formal inspection process, forwarding the request to an assigned Inspector. This Inspector will perform a double check and is equipped with the technical capability to reveal the identity of the pupil. The whole process will also be protocolled. This procedure guarantees that no single entity is able to arbitrarily spoil the privacy of the pupil and the identity is revealed in emergency cases only. If the School Inspection Board decides that the case does not require the identification of the user, it either closes

the case or may decide to delete the content and/or write a warning to the respective Restricted Area.

Who is involved in the trial?

- Teachers and other school personnel (also called staff)
- Pupils of grades 7, 8, 9 (all – A,B,C,D), excluding ones whose parents refused their children to participate in the pilot
- Guardians of pupils who participate

The total quantity of users in this pilot is more than 800 people. The participation in the trial is **free and voluntary**. In case the pupil of the class targeted for the trial wishes to participate, he/she can ask questions at any point in time by directing the enquiries to a contact person which is named below.

How does one participate in the pilot?

For the duration of the trial, the pupils as well as the involved school staff will receive a set of credentials which will be stored on a smart card provided by the school. The participants will receive the credential smart card together with an appropriate card reader to connect with the person's own personal computer at home or with a PC at the school. The credentials on the smart card are protected by a PIN known only to the participant. Thus, the participant will receive the following requisites for the pilot:

- Smart card
- One-time password for the smart card (PIN)
- Card Reader

With the credentials stored on the smart card, the pupils will be able to identify themselves for access to restricted chat rooms and restricted information in the IT system provided for the school. Thereby, they will be able to remain anonymous when asking private and sensitive questions from school personnel. But also, the school personnel can ensure that it communicates with the right authorized pupils of the respective school, gender, age or form. Moreover, the school personnel will be able to use their own credentials to set up chat rooms, online forums, document sharing areas, and polls to be used by a certain set of users (e. g. all children from class 7, only children age 13, only boys etc.). Also, school staff with correlating roles may also set up restricted and protected counselling sessions for the pupils (e. g. counsellors, social workers, nurses, coaches).

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 to use a many-step procedure to enter a school site. Whenever a

participant wants to access a certain IT service provided for the school (as mentioned above), the integrated ABC system provides an online interface between the browser and her smart card. For this reason, it employs a software component called “User Client” that runs locally on the user’s PC. This software component is triggered every time a participant is required to provide data stored on her card and asks for consent. Moreover, it enables the pupil to browse, delete, or locally backup the Privacy-ABCs stored on the own smart card. A number of card readers will also be available in the school, connected to common computers. For more in-depth explanation and help regarding the handling of the smart card, the User Client software, how to obtain credentials or to participate in school internal IT services, please refer to the pilot handbook available at the pilot’s portal page: www.abc4trust.se

What happens with the personal data?

For the usage of the school internal IT services as described above, the following personal information from the participants will be used within the pilot:

- First name
- Last name
- School
- Class
- Gender
- Date of birth
- Subject (meaning individual school courses, such as maths, English, physics etc.)

The named data is securely stored in a School Registration System which is run and administered by the ABC4Trust project partner Eurodocs. The processing is necessary for the purpose of issuing respective credentials to be stored locally on the smart cards of the participants and to re-issue credentials in case of lost cards. In addition, access to this data may become necessary for Eurodocs to ensure and measure the functionality of the pilot system and for tracking and remove errors.

Participants have the possibility to access and rectify data stored in the School Registration System online, or by contacting Eurodocs or the school. Eurodocs is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN), Munich, Germany, in setting up, running, and administering the School Registration System. For this it may become necessary to grant employees of NSN physical or online access to the School Registration System for administration purposes, validation of the system’s functions as well as tracking and removing of errors.

To protect the participant’s personal data, precautions have been made. NSN can only access the system under the supervision of Eurodocs. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by Eurodocs employees or online. In this case, the personal data underlies the same security requirements as if it would reside with the school. Any communication between NSN and the School Registration System will be protected against unauthorized access by third parties. Retrieved credentials are stored on the smart card under the control of the participant and accessible only with the PIN which will be handed out to the participants. **All personal information provided by**

the participating pupils will be treated carefully and confidentially. It will be stored securely and will not be used or disclosed to third parties without the pupil's and their parent's explicit consent. Since this pilot is part of scientific research project, aggregated and anonymised data will be used to complete the research work of this project as well as it will be used for academic purposes, like the publication of scientific proceedings; for drafting various informative reports, containing presentations of graphs and statistics that will be publicly available. The personal data in the collected, stored and processed will be deleted 6 months after the end of the trial.

User consent and effect of not consenting

The processing of personal data in this pilot falls under the scope of the Swedish protection law. To lawfully process this data, the school needs an informed consent of each participant. A consent form is attached to this information sheet.

All participants are free to give consent and an already provided consent may be revoked any time by notice towards the school. Not providing consent or revoking it later will not cause any disadvantages in class. Please note that without giving consent, the person may not participate in the trial.

Contact details of the responsible parties for questions and other inquiries:

Norrtullskolan, Norrtullsgatan 13, Söderhamn, Goran.Hanell@soderhamn.se, 0270-75759

Eurodocs AB, S:a Hamngatan 50, 826 50 Söderhamn, sosso@eurodocs.net, 070-5 742 742

More information about the project can be found at: www.abc4trust.eu

More information about the ABC system can be found in the user manual at: www.abc4trust.se/portal/help/usermanual

Come and join our school pilot – we'd be happy to welcome you and your participation in the ABC4Trust pilot trial!

Sincerely yours,

Norrtullskolan and Eurodocs

B.4 Consent form for school staff - English version



Consortium of the EU/FP7 programme-funded Research project ABC4Trust

Name & address of school partner

Consent form for the ABC4Trust Söderhamn pilot participation

This consent form addresses you as a participant in the first trial of a Privacy-ABC system at the Norrtullskolan within the EU-funded research and development project ABC4Trust. During this trial, the participant's personal data will be collected, stored and processed by the Eurodocs. For this, Norrtullskolan kindly asks you for your written consent to process the said personal data. For an explanation of the system deploying Privacy-ABCs that will be tested and the type of personal data processed for which purposes, please refer to the information sheet handed out as attachment to this form. Further information about the technical specifics can be found under the project website (www.abc4trust.eu), and especially in the user manual that is provided online at: www.abc4trust.se/portal/help/usermanual.pdf

Inter alia, this personal information will be processed during the trial:

- First name
- Last name
- School
- Class
- Gender
- Date of birth
- Subject (e. g. maths, English, physics etc.)

Beyond these bits of personal data used to enable the creation of the credentials and correlating accesses to the system, other personal data may find its way into the system through the content uploaded by the participants themselves, e.g. in the forums. Eurodocs is assisted by ABC4Trust project partner Nokia Siemens Networks Management International GmbH (NSN), Munich, Germany, in setting up, running, and administering the School Registration System (data processor). For this it may become necessary to grant employees of NSN physical or online access to the School Registration System for administration purposes, validation of the system's functions as well as tracking and removing of errors. To protect the participant's personal data, precautions have been made. NSN can only access the system under the supervision of Eurodocs. It will be avoided to transfer personal data to NSN (Germany), unless such transfer becomes necessary for troubleshooting tasks that cannot be done locally by Eurodocs employees or

online. In this case, the personal data underlies the same security requirements as if they would reside with the school. Any communication between NSN and the School Registration System will be protected against unauthorized access by third parties. In accordance with the principles of the Swedish Personuppgiftslagen (PUL) (<http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/>), all personal information provided by the participating pupil and related parents will be stored securely and will not be used or disclosed to third parties without explicit consent to do so. The participation in this trial will be completely confidential and personal data will be averaged and reported in aggregate. The personal information provided while using the above described services will only be used for the completion of this research project; in aggregated (i. e. anonymised) form for academic purposes, like the publication of scientific proceedings; for drafting various informative reports, containing presentations of graphs and statistics that will be publicly available. If any questions about these procedures remain, please refer to the responsible person at Norrtullskolan, Göran Hånell for any further inquiry or explanation. If the participating pupil does not wish to complete this trial, we kindly ask to inform Göran Hånell and he/she will facilitate the withdrawal from the trial. Not consenting or revoking consent does not have negative implications on a participation in class. This consent form will be securely kept with Norrtullskolan until 6 months after the end of the project.

Please express your consent regarding the above described trial participation below:

- By signing this consent form below, I indicate that I have read and understood the terms and conditions of the trial.
- **As part of the school personnel**, I hereby explicitly consent to voluntarily participate in the trial under the above described terms.

The explicit expression of consent includes the later usage of the collected and processed personal data in aggregated (i. e. anonymised) form for scientific research aimed at improving the Privacy-ABC technology and for correlating research and dissemination publications.

Date :

Name of participant :

Signature of participant :

Please give the signed consent form to: Göran Hånell

Contact information: Norrtullskolan, Norrtullsgatan 13, Söderhamn,

Goran.Hanell@soderhamn.se, 0270-75759

Goran.Hanell@soderhamn.se, 0270-75759

B.5 Legal Notice and privacy policy of the website - English version



Legal Notice

This website is the information and access portal for the participants of the Söderhamn school pilot in the ABC4Trust ICT research and development project. It is provided by members of the ABC4Trust consortium, and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the website or the information, products, services, or related graphics contained on the website for any purpose. The information in this website is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Every effort is made to keep the website up and running smoothly. However, the ABC4Trust consortium takes no responsibility for, and will not be liable for, the website being temporarily unavailable due to technical issues beyond our control.

Through this website, you are able to access other websites (e.g. via the Portal buttons and links) which are not under the control of the ABC4Trust consortium. We have no control over the nature, content and availability of those sites. The inclusion of any links does not necessarily imply a recommendation or endorse the views expressed within them. So please be aware that the ABC4Trust consortium is not responsible for the content and the privacy practice of such other sites. We encourage our users to be aware when they leave our site and to read the privacy policy of these third party sites. The following Privacy Policy applies solely to this web portal of the ABC4Trust consortium.

Privacy Policy

This is a privacy policy for the ABC4Trust website. This website falls under the responsibility of the ABC4Trust consortium. It is concerned with the dissemination and exchange of information about the ABC4Trust research project as well as giving the pilot’s participants access to the Privacy ABC System they have agreed to test. It is not concerned with commercial transactions or with the exchange of data for marketing purposes. The ABC4Trust website does not work with any third party that serves ads to this site.

Concerning traffic data which is created by browsing the web portal, we do not store personal data of the users. Personally identifiable information like IP addresses are not stored after the delivery of the web page. We only store and use anonymous data on the used browser type for statistical means to administer this web portal. These data are not linked to a name, a Cookie, an IP address or another unique identifier. No registration is required to access the main site of this web presence.

The abc4trust.se portal website does not retain IP-addresses. For abc4trust.se and portal.abc4trust.se cookies containing the language code are used if the language selector is set to another language as Swedish. The subpage idm.abc4trust.se uses session cookies to issuing credentials to a previously identified user.

During access to our site, specific data are stored in log-files. These data cannot be related to individual persons. In detail the data stored are:

- Name of the requested file
- Date and time of request
- Data-volume of request
- Message if transmission was successful

The log-files are used for statistical purposes only. Under no circumstances they are passed on to third parties.

The user has the right to request at any time information about the stored personal data. She has the unrestricted right of deletion, updating and correction of the stored personal data unless required otherwise by the applicable law. This can e.g. be done by sending an e-mail to: privacy@abc4trust.eu

If we decide we need to change our privacy policy, we will post those changes this website, so our users are always aware of what information we collect, how we use it, and under circumstances, if any, we disclose it.

We invite you to contact us if you have questions about this policy at: privacy@abc4trust.eu

Contact

Eurodocs AB

Södra Hamngatan 50

826 50 Söderhamn

Info@eurodocs.net

© ABC4Trust 2013

Appendix C User Manual

The following is included in the pages that follow.

C.1 User Manual – Söderhamn round 1 – English version

C.1 User Manual - Söderhamn round 1 - English version

The following user manual in English is from the first round of the pilot. The user manual from the second round of the pilot exists only in Swedish. The following is a scanned version of the User Manual. For a high quality original version of the User Manual in Swedish used for the second round please visit <http://bit.ly/1fEle1q>



User Manual
Söderhamn pilot, round 1
English version



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.

ABC4Trust

Table of Contents

1	How to start?	6
1.1	How to get your Smart Card	6
1.2	How to Setup Your PC	7
1.3	Smart Card User Interface	12
1.4	How to Register Your Smart Card	14
1.5	How to Obtain a School Credential	25
1.6	How to Obtain All Credentials	31
1.7	How to View Your Credentials	36
2	Use the Restricted Area Application	39
2.1	How to login to Application	39
2.2	Main controls of Application	43
2.3	How to use Alias Selector	46
1.1.1	Create new Alias	46
1.1.2	Use the Alias	49
2.4	How to use the Dashboard	50
2.5	How to Search for and Enter the Restricted Area	51
2.6	How to use Wall	54
2.7	How to use Documents	56
2.8	How to use Chat	56
3	Additional Features	57
3.1	How to Revoke or change Credentials	57
3.2	How to Backup Your SC's Data	57
3.3	How to Restore SC's Data	60
3.4	How to Change Your PIN	63
3.5	How to Unlock Your Smart Card	66
3.6	How to use Inspection	68
4	Contacts	70

ABC4Trust

Index of Figures

Figure 1 ABC4Trust Smart Card.....	6
Figure 2 Smart Card Reader.....	7
Figure 3. PIN and PUK from letter.....	7
Figure 4 One-time password.....	7
Figure 5 Card Reader.....	8
Figure 6 Update manager.....	8
Figure 7 First step of setup.....	9
Figure 8 Installation Process.....	9
Figure 9 Finish Setup.....	10
Figure 10 Firefox plugin installation.....	11
Figure 11 Restart Firefox after install.....	11
Figure 12 Enter PIN code.....	12
Figure 13 Request to use Smart Card Credentials.....	13
Figure 14 Make selection.....	14
Figure 15 Place Smart Card.....	15
Figure 16 Follow Get Credentials link.....	15
Figure 17 IDM.....	16
Figure 18 Login with civic reg.# and OTP.....	17
Figure 19 Login welcome message.....	18
Figure 20 Attributes List.....	18
Figure 21 Register Card.....	19
Figure 22 Enter PIN.....	19
Figure 23 Credential Selector.....	20
Figure 24 Close the waiting window.....	21
Figure 25 Successful verification message.....	22
Figure 26 Card registered.....	22
Figure 27 Logout from IdM.....	23
Figure 28 Failed Enter with OTP.....	24
Figure 29 Clean cookies.....	24
Figure 30 Get Credentials.....	25
Figure 31 IdM welcome screen.....	26
Figure 32 Login with token.....	27
Figure 33 PIN Authentication.....	27
Figure 34 CredSchool page.....	28
Figure 35 Click Get Credential to obtain credSchool.....	29
Figure 36 Smart Card dialog.....	30
Figure 37 Verification OK.....	30
Figure 38 School Credential obtained.....	31
Figure 39 Get Credentials.....	32
Figure 40 Login to IdM.....	32
Figure 41 Login with token.....	33
Figure 42 PIN Authentication.....	33
Figure 43 CredSchool page.....	34
Figure 44 Get credentials.....	34
Figure 45 Credentials written to the card.....	35
Figure 46 Credential obtained.....	35
Figure 47 Verification failed.....	36

ABC4Trust

Figure 48 Web Browser menu.....	37
Figure 49 List credentials.....	37
Figure 50 Enter PIN.....	38
Figure 51 List of credentials.....	38
Figure 52 Click to navigate to the Restricted Area Application.....	39
Figure 53 RA Welcome Screen.....	40
Figure 54 Enter PIN.....	40
Figure 55 Create first alias.....	41
Figure 56 Choose existing alias.....	41
Figure 57 List of RA.....	42
Figure 58 Main menu.....	43
Figure 59 Credential Selector.....	43
Figure 60 Create Area.....	44
Figure 61 Restricted Area example.....	45
Figure 62 Open Alias Selector.....	46
Figure 63 Click "New" to create Alias.....	47
Figure 64 If alias exists, you will get an error.....	47
Figure 65 If Alias can be created, Smart Card UI will popup.....	48
Figure 66 After creation alias will appear in list. Click save to use new Alias, Smart Card UI will popup.....	48
Figure 67 New Alias is at use.....	49
Figure 68 Click on Alias to call Alias Selector.....	49
Figure 69 Interact with Smart Card.....	50
Figure 70 See the Alias at use.....	50
Figure 71 Click on "Home" link to open dashboard.....	51
Figure 72 Main menu on top of this image.....	52
Figure 73 Click "Enter".....	52
Figure 74 Access Policy Details.....	53
Figure 75 Smart Card Interface described in Chapter 3.3.....	53
Figure 76 Successfully entered the Restricted Area.....	54
Figure 77 General view on wall.....	55
Figure 78 Add content to the wall.....	56
Figure 79 Web Browser menu.....	57
Figure 80 ABC4Trust menu.....	58
Figure 81 Click "Continue".....	58
Figure 82 Notification.....	59
Figure 83 Smart Card PIN entry.....	59
Figure 84 Choose password.....	59
Figure 85 Backup success.....	60
Figure 86 Web Browser menu.....	61
Figure 87 Restore Smart Card.....	61
Figure 88 Notification.....	62
Figure 89 Check the PIN.....	62
Figure 90 Enter the password from backup.....	62
Figure 91 Success message.....	63
Figure 92 Web Browser menu.....	64
Figure 93 Notification.....	64
Figure 94 Enter PIN.....	65
Figure 95 Enter new PIN.....	65
Figure 96 Success message.....	65
Figure 97 Web Browser menu.....	66
Figure 98 Choose Unlock card.....	67
Figure 99 Notification message.....	67

ABC4Trust

Figure 100 Enter PUK.....	68
Figure 101 Enter new PIN.....	68
Figure 102 New PIN was chosen.....	68

ABC4Trust

1 How to start?

1.1 How to get your Smart Card

Please contact teacher responsible for classroom to get the guidance in order to retrieve the card and other requisites.

For the next step you will need:

- Smart Card initialized with secret key and given by School Administrators
- Letter with Card Number, PIN and PUK code



Figure 1 ABC4Trust Smart Card

ABC4Trust



Figure 2 Smart Card Reader

DeviceID	pin	puk
35	4220	48520787

CARD#	PIN	PUK
1234	1234	12345678

Figure 3. PIN and PUK from letter

SMART CARD #1234
NAMN: LEIF OLOFSSON
PERSONNUMMER: 661111-1234
LÖSENORD: R7HJ#1J

Figure 4 One-time password

1.2 How to Setup Your PC

In order to Setup the PC following steps must be done:

- Make sure your computer software is matching minimal requirements for pilot
- Launch Mozilla Firefox or Internet Explorer

ABC4Trust

- Install User Service using installer from <http://abc4trust.se/Portal/help>
- Connect Smart Card Reader to computer
- Visit the School Portal on <http://abc4trust.se>

Now step by step!

Step 1

Plug the USB cable of Card Reader to the PC



Figure 5 Card Reader

Step 2

Wait for installation of drivers as shown in the image below

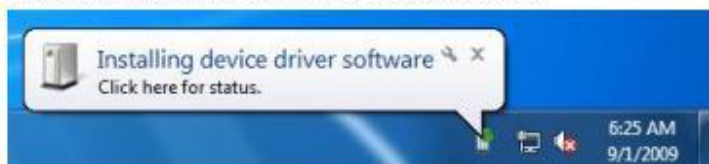


Figure 6 Update manager

Step 3

Please visit the School Portal, "Help & Downloads" section (<http://abc4trust.se/Portal/help>) and download the ABC4Trust User Service Installer.exe

Step 4

Launch the installer and go through all steps until the finish.

ABC4Trust



Figure 7 First step of setup

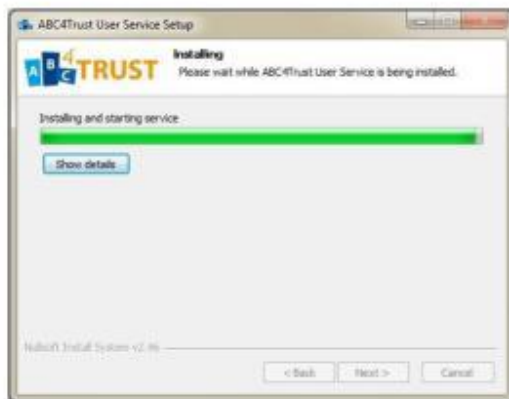


Figure 8 Installation Process

ABC4Trust

**Figure 9 Finish Setup****Step 5**

After this process is finished you should have installed two components:

1. Firefox / Internet Explorer Plugins
2. Local ABC4Trust Service (needed to work with Smart Card)

Step 6

Now we have to check if browser plugin was set up successfully (on example of Firefox).

1. Restart Firefox and you will get the screen like Figure 10 Firefox plugin installation
2. Then please select the corresponding tab as shown in order to accept ABC4Trust User service's installation.
3. Now, continue the installation and restart your browser (Figure 11 Restart Firefox after install)

ABC4Trust

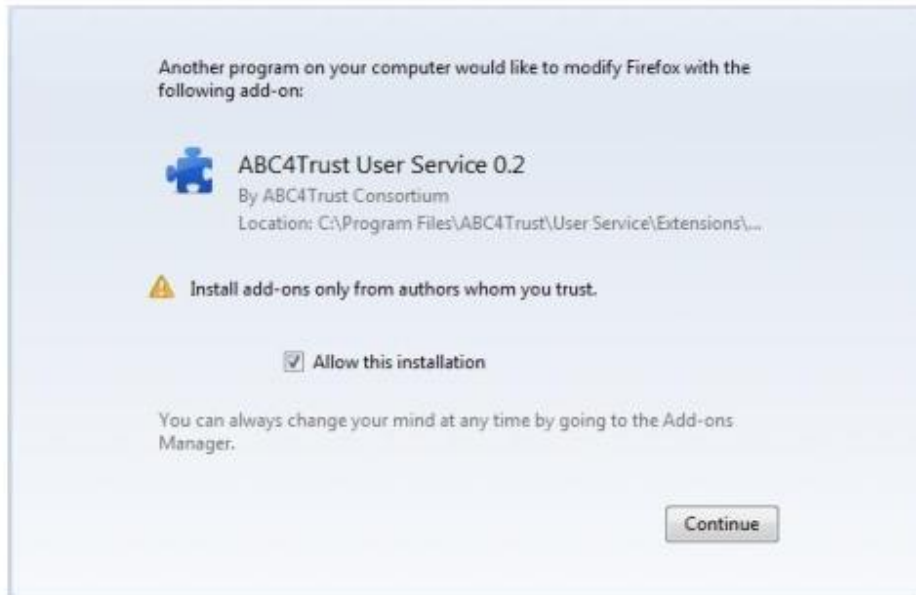


Figure 10 Firefox plugin installation



Figure 11 Restart Firefox after install

ABC4Trust

Troubleshooting

If you cannot see the windows update manager notification figure (Figure 6 Update manager), you have to restart your pc with your smart card connected to your computer via your reader, as the Figure 5 Card Reader, shows.

If you cannot see the plugin at your Firefox browser, as Figure 10 Firefox plugin installation, shows please restart your browser. If the plugin notification is still missing, you have to repeat the setup procedure from the beginning.

If the ABC4Trust User Service is NOT running at the services menu, as **Fel! Hittar inte referensskälla.** shows.

1. Please restart your pc and repeat the above Step 7.
2. If the ABC4Trust User Service is not running, you have to uninstall the ABC4Trust User Service and repeat the setup procedure from the beginning.

1.3 Smart Card User Interface

Your Smart Card contains your Credentials therefore it is a subject of additional security matters. Smart Card user service has protection with encryption and user interface to let user grant access to information on the card in a controllable and safe way.

Within any operations which requires information or check with a help of Smart Card there are several dialogs to let user manage operations.

Let's learn the typical scenario of interaction with Smart Card interface.

Step 1. Enter PIN code

In order to prove that you're an owner of the card and let the system to decrypt your data you have to enter your PIN code.



Figure 12 Enter PIN code

Please note that to make the comfort if your usage of the system better – PIN code is safely cached during one session of work with application, so this dialog might not appear if you have recently entered it.

Step 2. Request of Smart Card

While user performs the action which needs a Smart Card he will receive a popup which will ask to choose the source of credentials (your Smart Card).

ABC4Trust

It is recommended to keep Card in Card Reader and attached to computer all the time when you use and application – otherwise you will get errors.

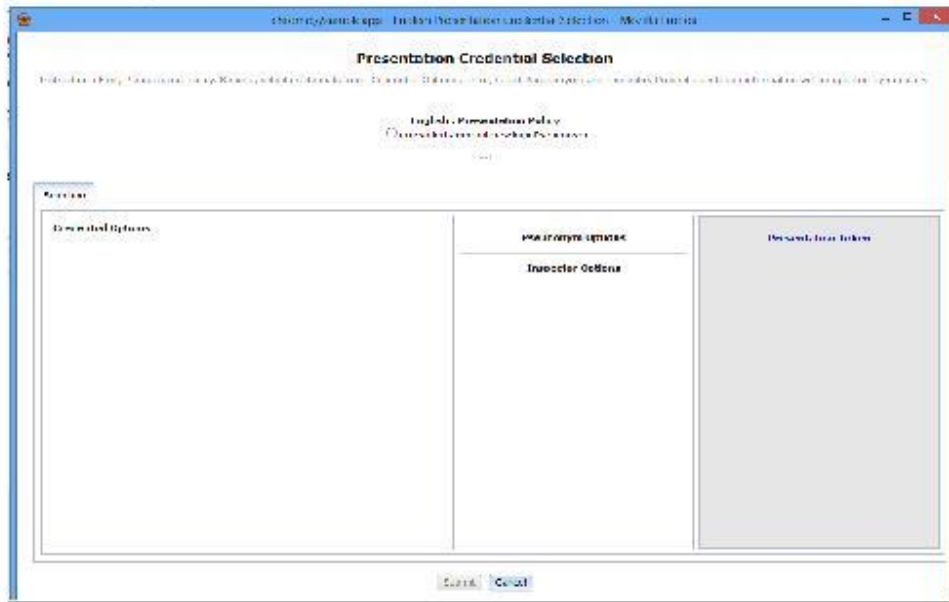


Figure 13 Request to use Smart Card Credentials

Step 3. Choose policy

Pseudonym is a unique card identifier which is serving as a key to encrypt data and keep them secure. It is obtain to the card while registering the Smart Card on IdM (How to Register Your Smart Card)

To choose a pseudonym simply choose the option on the top of popup, it is a Presentation Policy which includes the pseudonym.

ABC4Trust

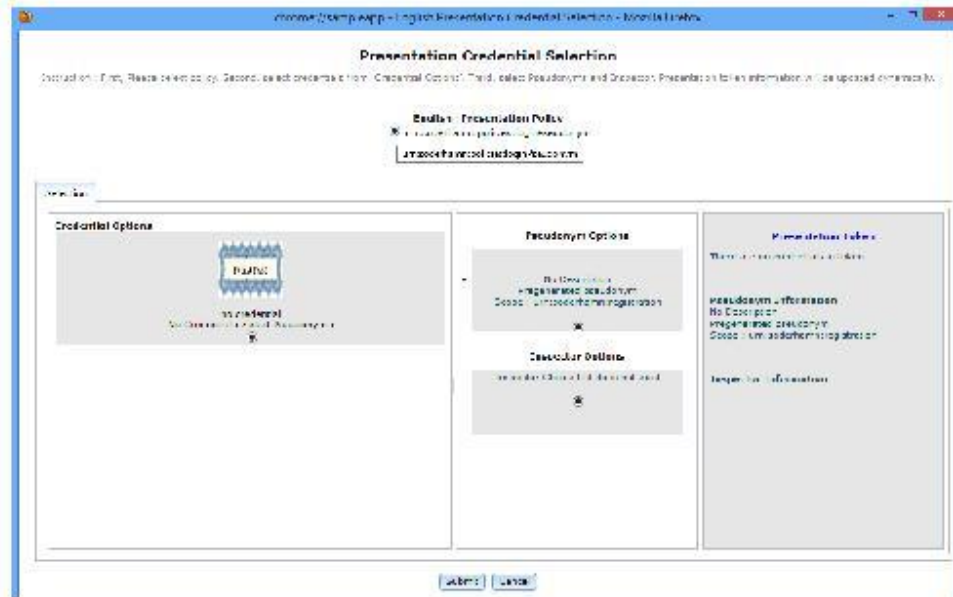


Figure 14 Make selection

Troubleshooting

In case of difficulties you might be interested in following parts of Chapter **Fel! Hittar inte referensskälla..**

1.4 How to Register Your Smart Card

Before reading this step, make sure you have successfully completed chapter "How to Setup Your PC"

Step 1

Plug the USB cable of card Reader to your computer and place the smart card into the card Reader as the figure below shows.

ABC4Trust



Figure 15 Place Smart Card

Step 2

Open web address of School Portal, then follow a link "Get Credentials" to access the Identity Manager (IdM)

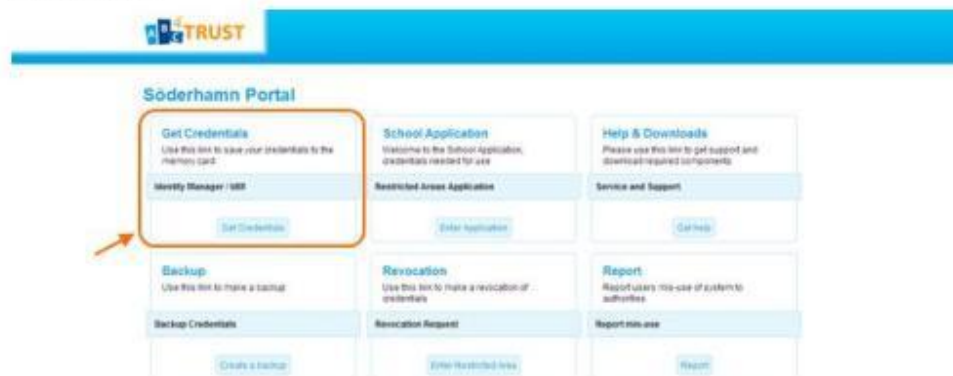


Figure 16 Follow Get Credentials link

ABC4Trust

Step 3

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



Figure 17 IDM

Step 4

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

ABC4Trust



Figure 18 Login with civic reg.# and OTP

In case if authentication failed on this step please check the **Troubleshooting** section at the end of Chapter.

Step 5

If the authentication is successful you will see a welcome message.

Now you can access your account information and all your attributes under the "Admin" menu (Figure 20 Attributes List). To continue with smart card registration click on "Register".

ABC4Trust



Figure 19 Login welcome message



Figure 20 Attributes List

ABC4Trust

Step 6

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



Figure 21 Register Card

Step 7

The ABC4Trust User Service application requests your PIN in order to unlock the card. Please enter your PIN in the corresponding box as following Figure shows and click the "OK" button.

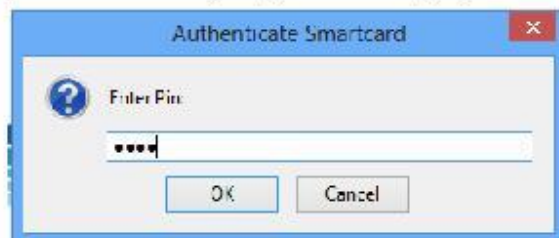


Figure 22 Enter PIN

Step 8

ABC4Trust

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

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

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

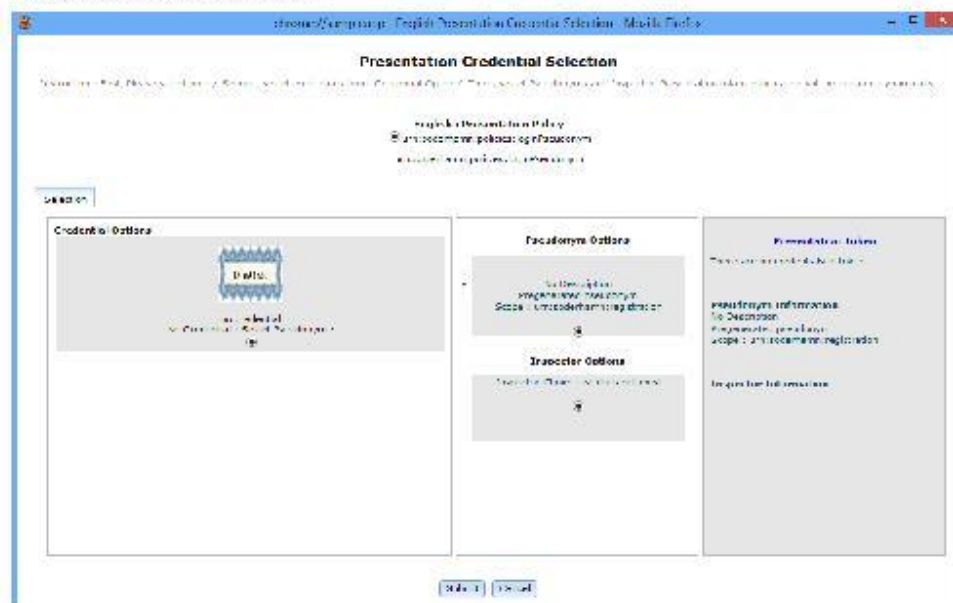


Figure 23 Credential Selector

ABC4Trust

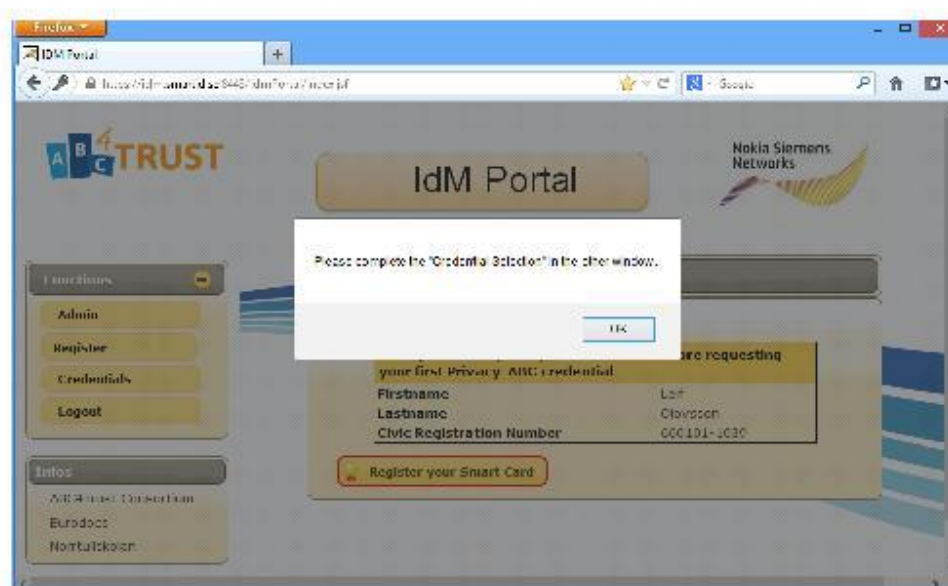


Figure 24 Close the waiting window

Step 9

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

ABC4Trust

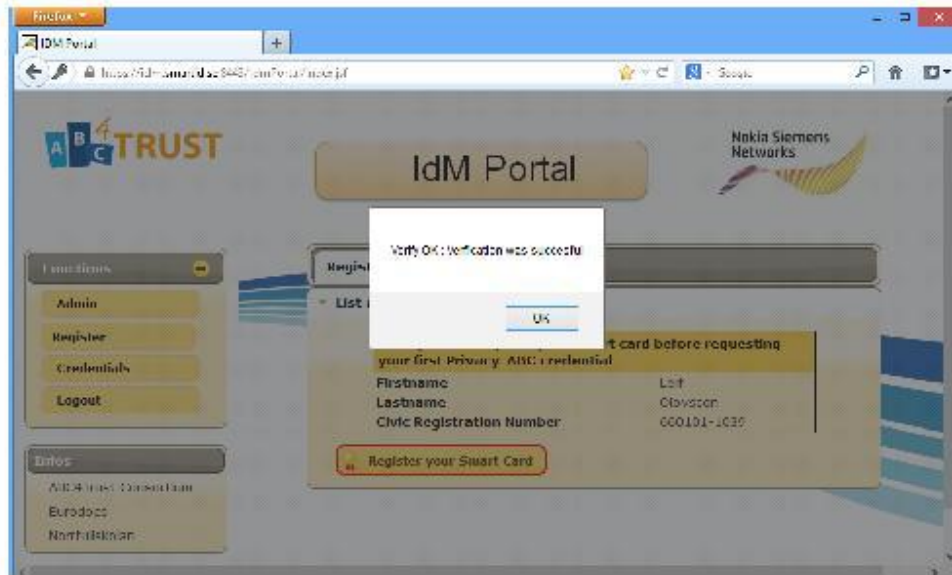


Figure 25 Successful verification message

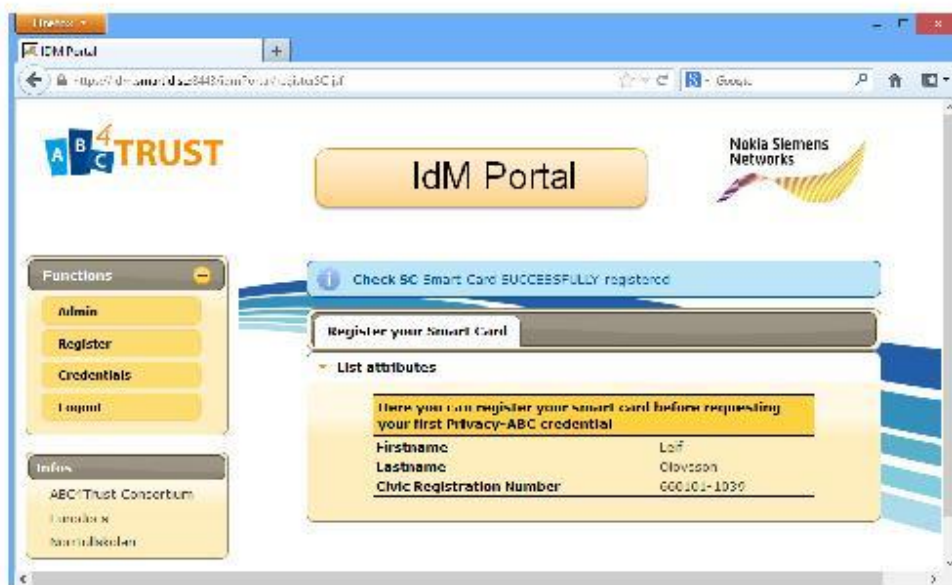


Figure 26 Card registered

ABC4Trust

Step 10

Now your smart card is registered and you can proceed with obtaining your credentials (How to Obtain a School Credential and How to Obtain All Credentials). To proceed with this step you have to Logout.

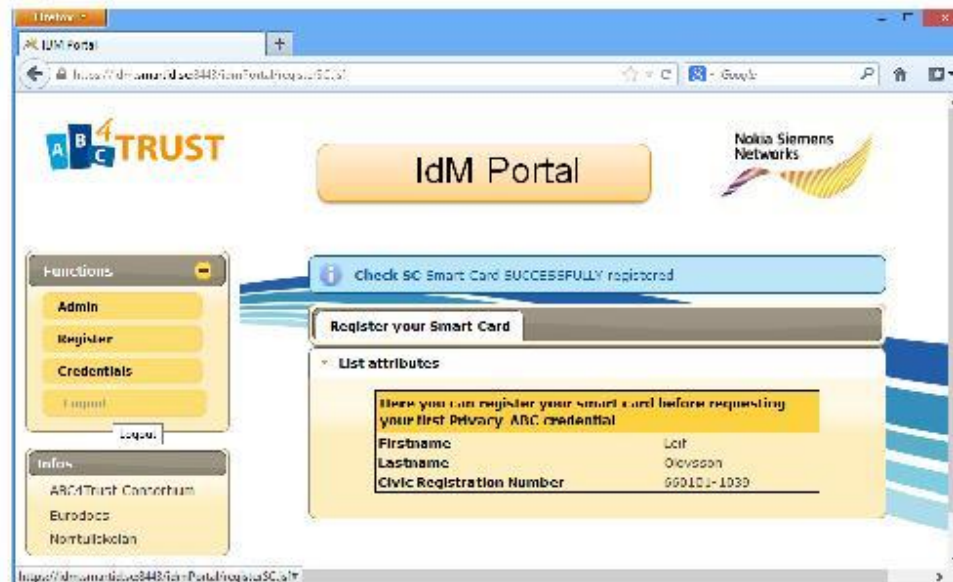


Figure 27 Logout from IdM

Troubleshooting the SC's Registration

ABC4Trust



Figure 28 Failed Enter with OTP

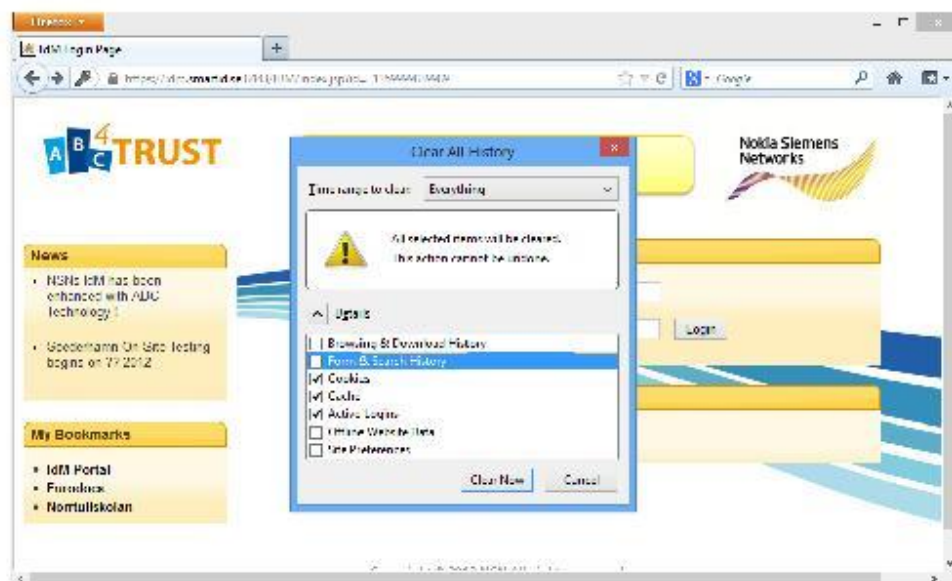


Figure 29 Clean cookies

If you cannot access your account at step 5, you have to check and reenter your OTP and your matriculation number.

ABC4Trust

If you cannot access credential selection menu at step 8, you have to check your smart card connection to your computer via your reader (as the Figure 15 Place Smart Card shows).

If you cannot receive system's authentication at step 9 or get an error message, you have to check your smart card connection to your computer via your reader (as the Figure 15 Place Smart Card shows).

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

1.5 How to Obtain a School Credential

Before proceeding current phase:

- When you want to register at the School Pilot and obtain a valid School credential, you have to complete successfully the above registration phase (see "How to Register Your Smart Card") and to possess a valid user Privacy ABC on his smart card.
- You must have installed the ABC4Trust service at your computer.
- You have to plug the USB cable of card Reader to your computer and place the Smart Card into the card Reader.

Step 1

Visit School Portal and choose "Get Credentials" to enter the Identity Manager (IdM)

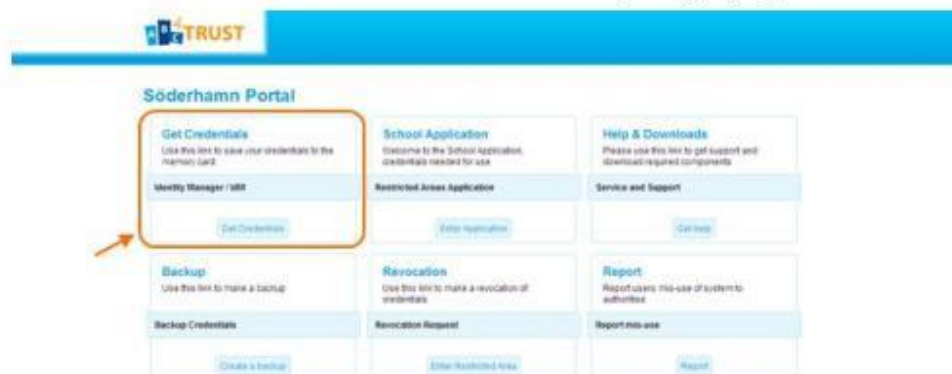


Figure 30 Get Credentials

Step 2

You are redirected to IdM portal, hit the "Login" link on the left

ABC4Trust

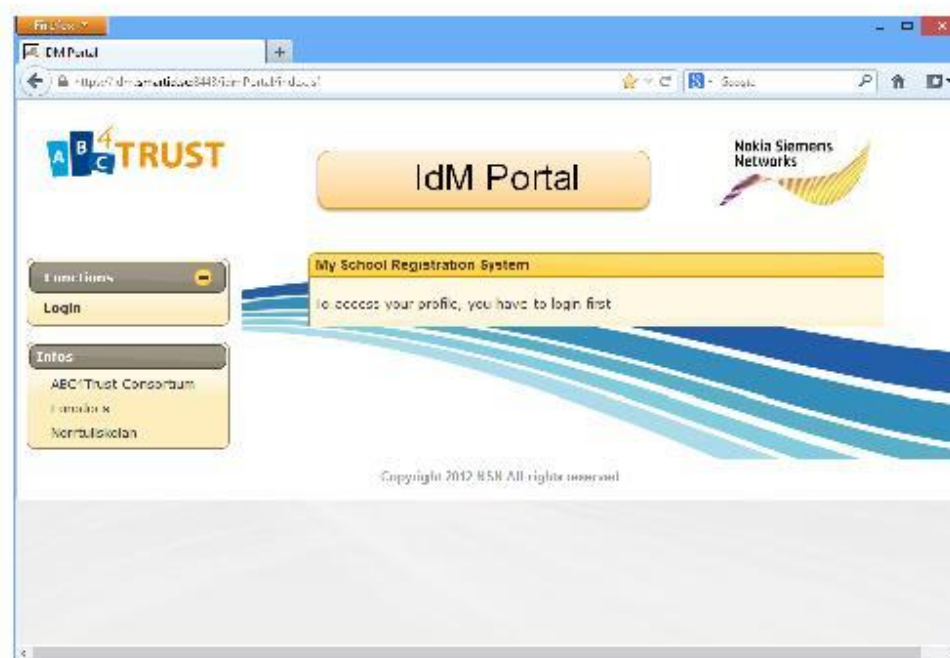


Figure 31 IdM welcome screen

Step 3

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

ABC4Trust



Figure 32 Login with token

Step 4

The ABC4Trust User Service application requests your PIN in order to unlock the card. Please enter your PIN in the corresponding box and click the “OK” button.

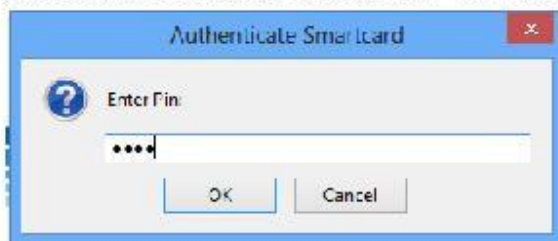


Figure 33 PIN Authentication

Step 5

If the authentication is successful you will see a welcome message. Now you can select “credentials” link in the functions menu of your account page.

ABC4Trust



Figure 34 CredSchool page

Step 6

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

ABC4Trust



Figure 35 Click Get Credential to obtain credSchool

Step 7

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

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

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

ABC4Trust

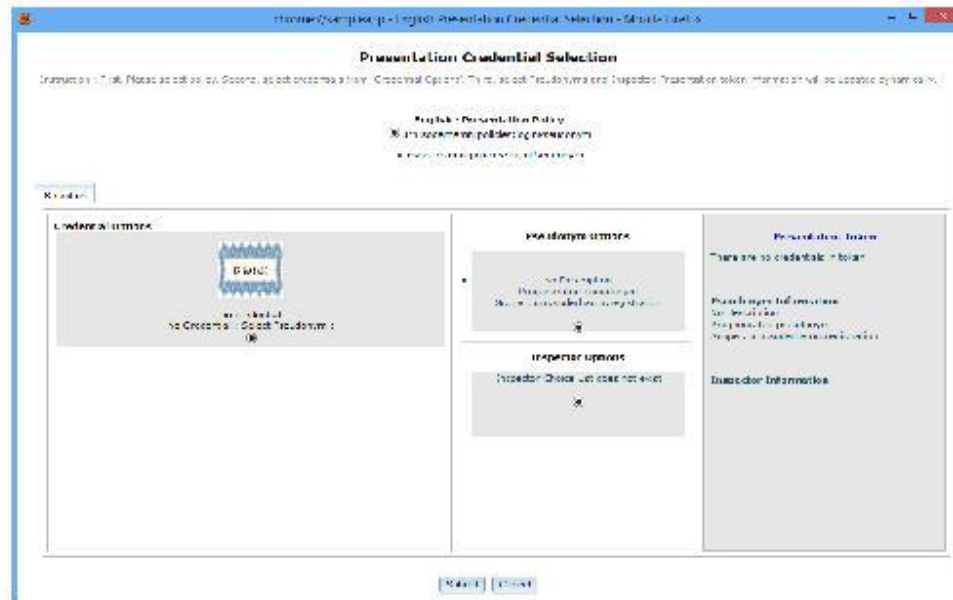


Figure 36 Smart Card dialog

Step 8

The System authenticates you by using the stored data in your smart card and if authentication is successful you will see a "Verification OK" message (see Figure 37 Verification OK). If your University credential is stored in your smart card your credential status will be appeared as shown in Figure 38 School Credential obtained. To verify that your credential was successfully stored on your card, click on the List Credentials menu on your Firefox browser (see "How to get your Smart Card").

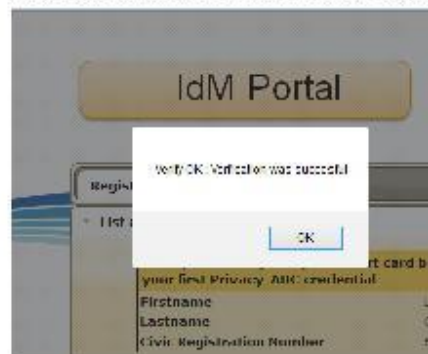


Figure 37 Verification OK

ABC4Trust



Figure 38 School Credential obtained

Troubleshooting

If you cannot access your account at step 5, you have to check your smart card connection to your computer via your reader as the Figure 15 Place Smart Card shows.

If you cannot receive system's authentication at step 8 or get an error message, you have to check your smart card connection to your computer via your reader as the Figure 15 Place Smart Card shows.

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

1.6 How to Obtain All Credentials

Please make sure these steps are completed before:

- When you want to book a course and obtain a valid course credential, you have to complete successfully the previous registration phase (see "How to Register Your Smart Card") and to possess a valid student Privacy ABC credential following the steps of obtaining a university credential phase (see "How to Obtain a School Credential").
- You must have installed the ABC4Trust service at your computer.
- You have to plug the USB cable of card Reader to your computer and place the smart card into the card Reader as the Figure 15 Place Smart Card shows.

Step 1

Visit School Portal and choose "Get Credentials" to enter the Identity Manager (IdM)

ABC4Trust

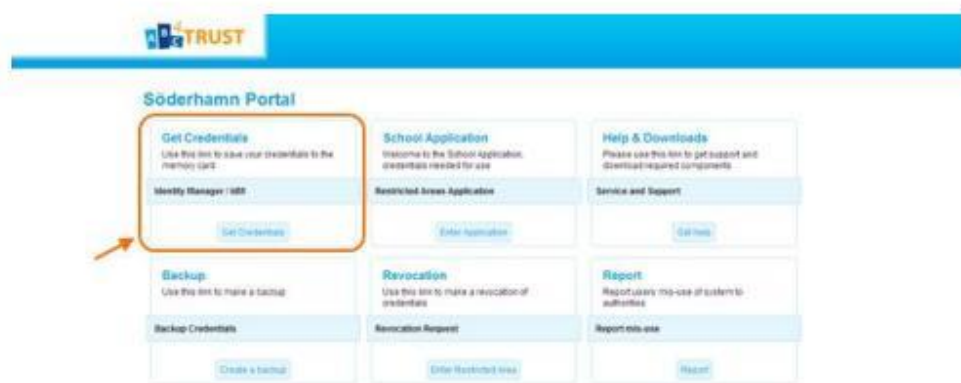


Figure 39 Get Credentials

Step 2

You are redirected to IdM portal, hit the "Login" link on the left



Figure 40 Login to IdM

ABC4Trust

Step 3

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



Figure 41 Login with token

Step 4

The ABC4Trust User Service application requests your PIN in order to unlock the card. Please enter your PIN in the corresponding box and click the "OK" button.



Figure 42 PIN Authentication

Step 5

If the authentication is successful you will see a welcome message. Now you can select "Credentials" link in the functions menu of your account page

ABC4Trust



Figure 43 CredSchool page

Step 6

On current stage you can choose what credentials have to be retrieved to the card, via choosing and appropriate tab.

Step 7

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

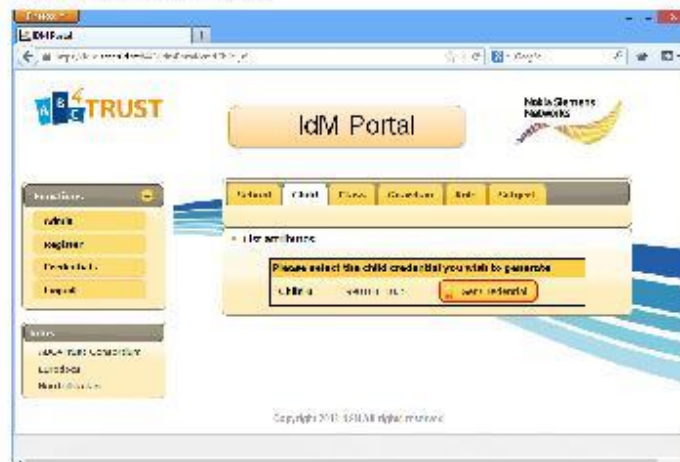


Figure 44 Get credentials

ABC4Trust

System will request access to the Smart Card as described in Chapter 1.3 Smart Card User Interface.

Step 8

If the operation was successful you will have a confirmation from IdM



Figure 45 Credentials written to the card

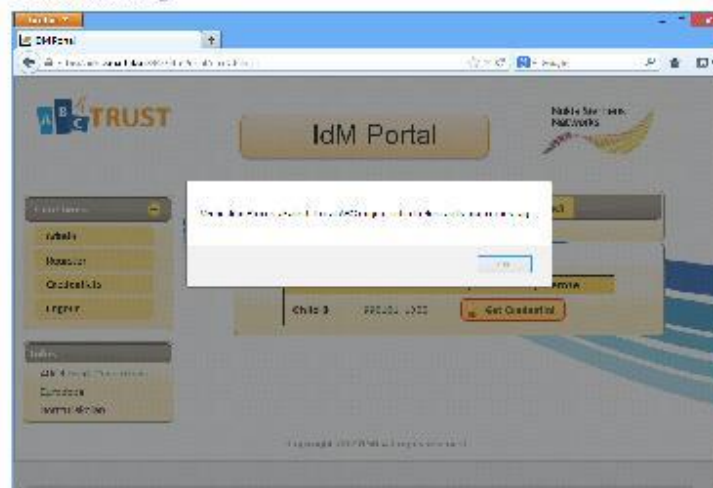
Step 9

The System authenticates you by using the stored data in your smart card and if authentication is successful you will see a "Verification OK" message (see Fel! Hittar inte referensskälla.). If your University credential is stored in your smart card your credential status will be appeared as shown in Figure 46 Credential obtained. To verify that your credential was successfully stored on your card, click on the List Credentials menu on your Firefox browser (see "How to get your Smart Card").



Figure 46 Credential obtained

ABC4Trust

Troubleshooting**Figure 47 Verification failed**

If you cannot access your account at step 5, you have to check your smart card connection to your computer via your reader as the Figure 15 Place Smart Card shows.

If you cannot receive system's authentication at step 8 or get an error message, you have to check your smart card connection to your computer via your reader as the Figure 15 Place Smart Card shows.

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

1.7 How to View Your Credentials

All Pilot users are able to see the Credentials they have on the card.

Smart Card is the only place where Credentials are available, users can retrieve them from IdM as explained in chapter 1.6.

To start the procedure please make sure that following is done:

- You have installed the ABC4Trust service at your computer.
- You have to plug the USB cable of card reader to your computer and place the smart card into the card reader as the Figure 15 Place Smart Card shows.

Step 1

Open your Firefox browser. You will see the following interface on your screen. Follow the tab "Tools" at your Firefox browser menu.

ABC4Trust

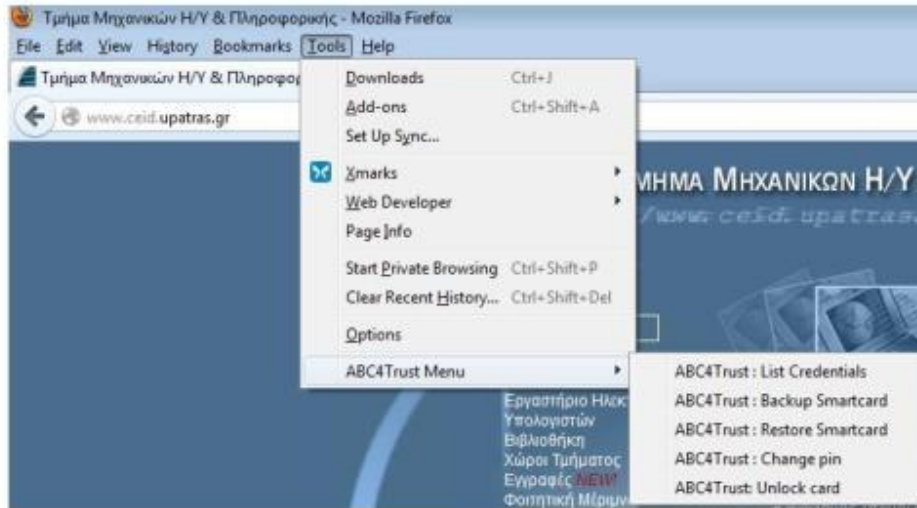


Figure 48 Web Browser menu

Step 2

Now select the “ABC4Trust Menu” tab under the Tools Menu and choose item “List credentials” as shown below

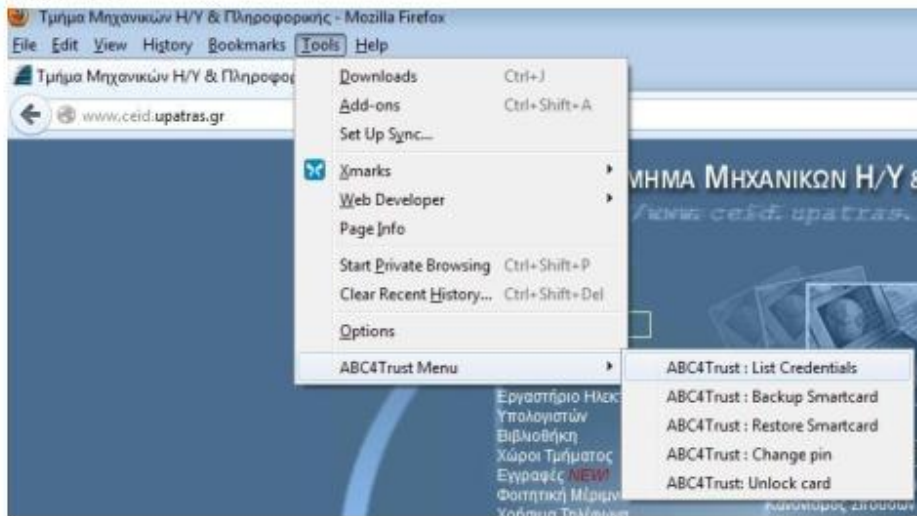


Figure 49 List credentials

ABC4Trust

Step 3

Now, please enter your PIN in the corresponding box and click the "OK" button.



Figure 50 Enter PIN

Step 4

Now you will be able to see the following interface which shows your stored credentials on your smart card.

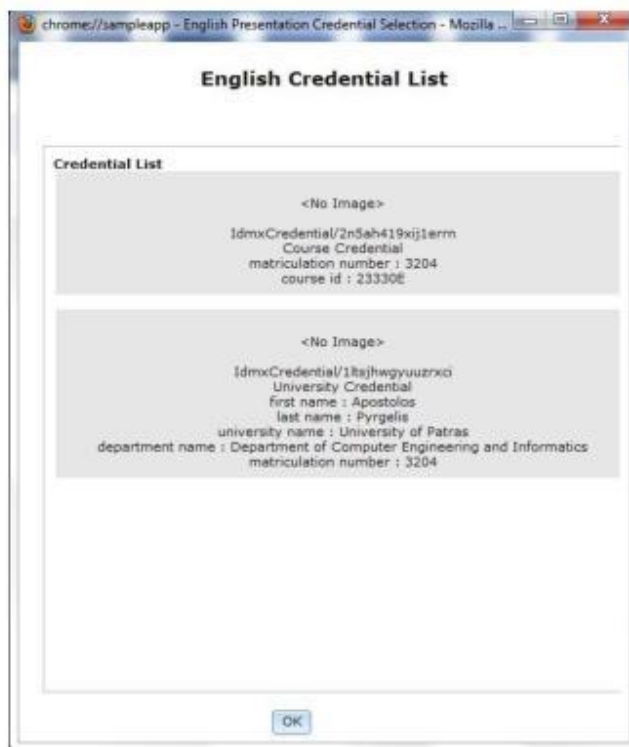


Figure 51 List of credentials

ABC4Trust

2 Use the Restricted Area Application

2.1 How to login to Application

In order to login to Restricted Area Application (also called School Application), user have to navigate from the School Portal using link “Enter RA Application”. Link to the Restricted Area Application can be placed in bookmarks to avoid coming back to School Portal if only access to this application will be needed.



Figure 52 Click to navigate to the Restricted Area Application

ABC4Trust

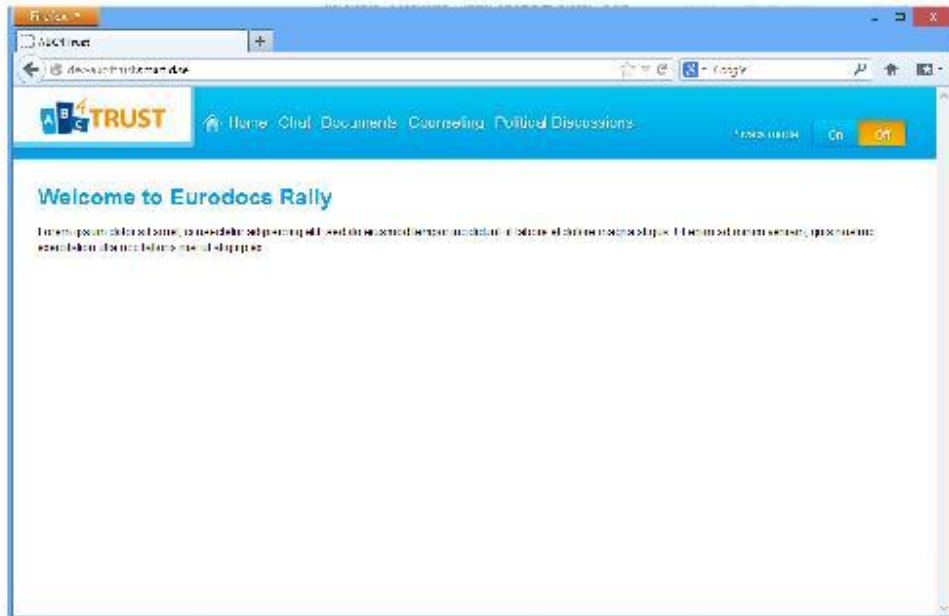


Figure 53 RA Welcome Screen

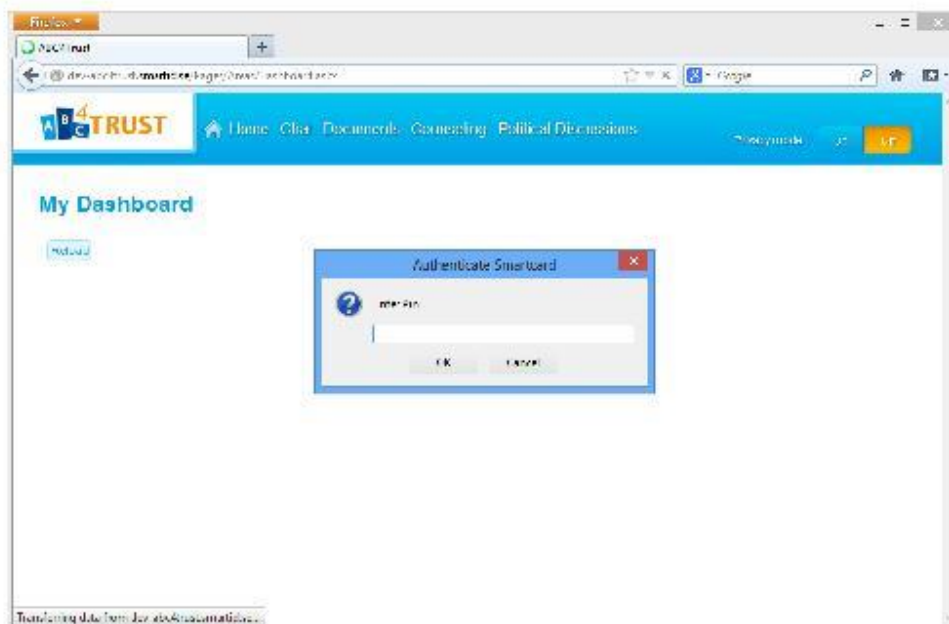


Figure 54 Enter PIN

ABC4Trust

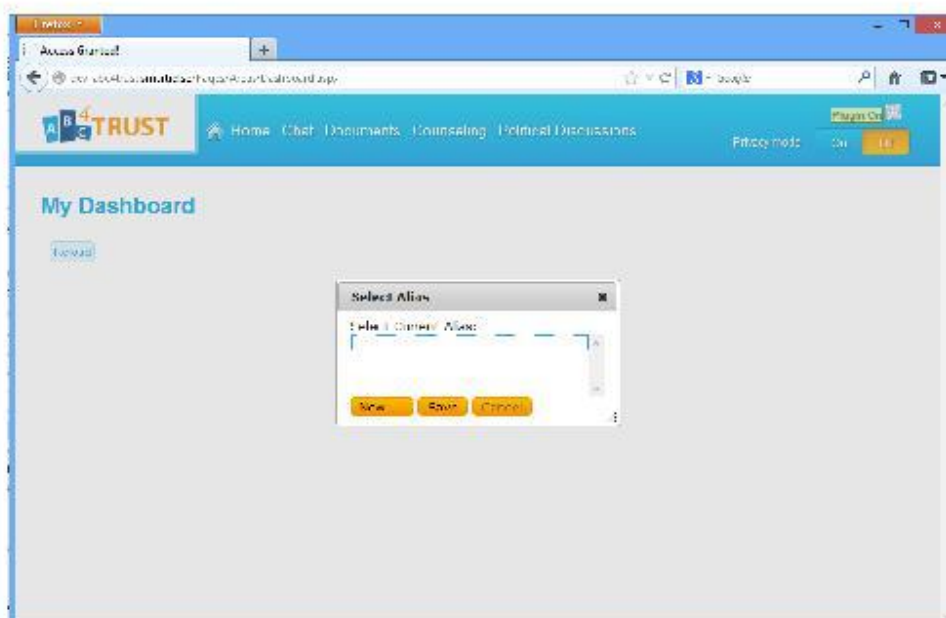


Figure 55 Create first alias

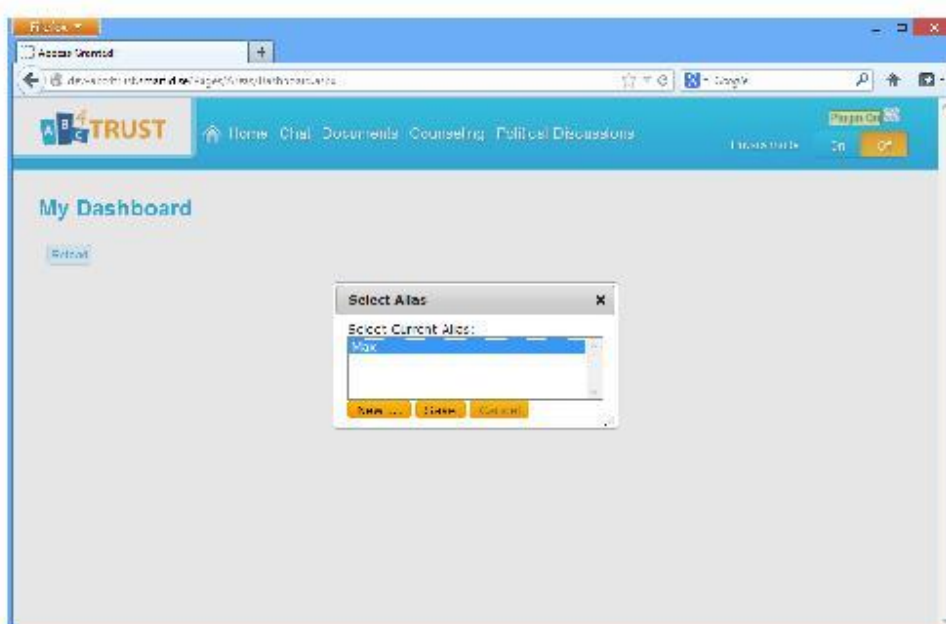


Figure 56 Choose existing alias

ABC4Trust

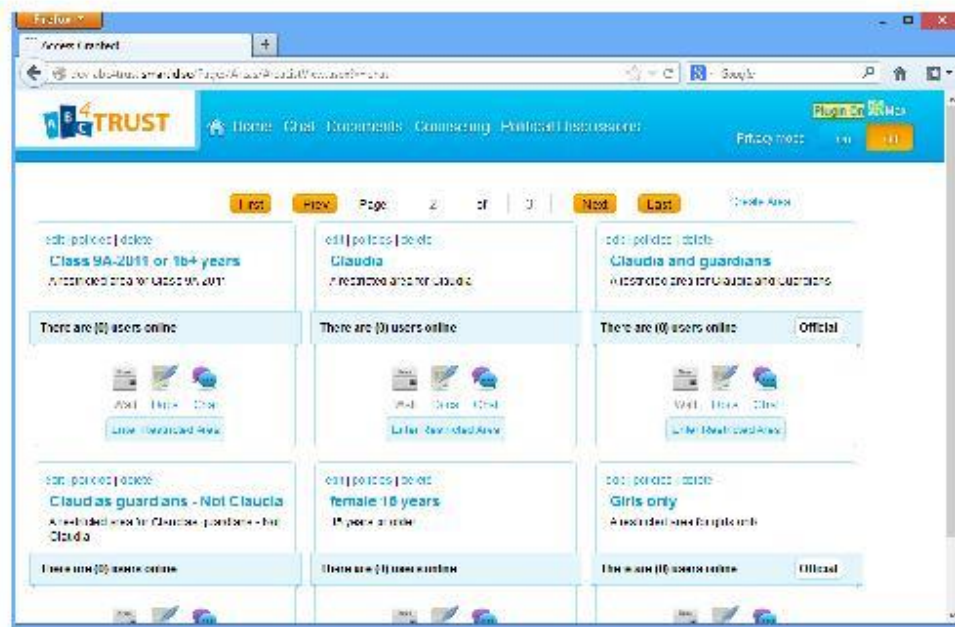


Figure 57 List of RA

ABC4Trust

2.2 Main controls of Application

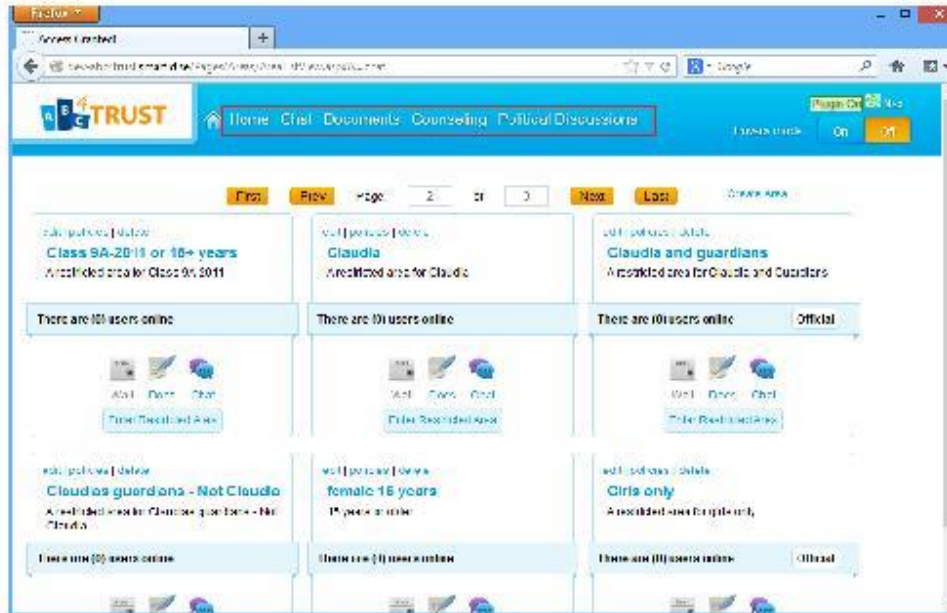


Figure 58 Main menu



Figure 59 Credential Selector

ABC4Trust

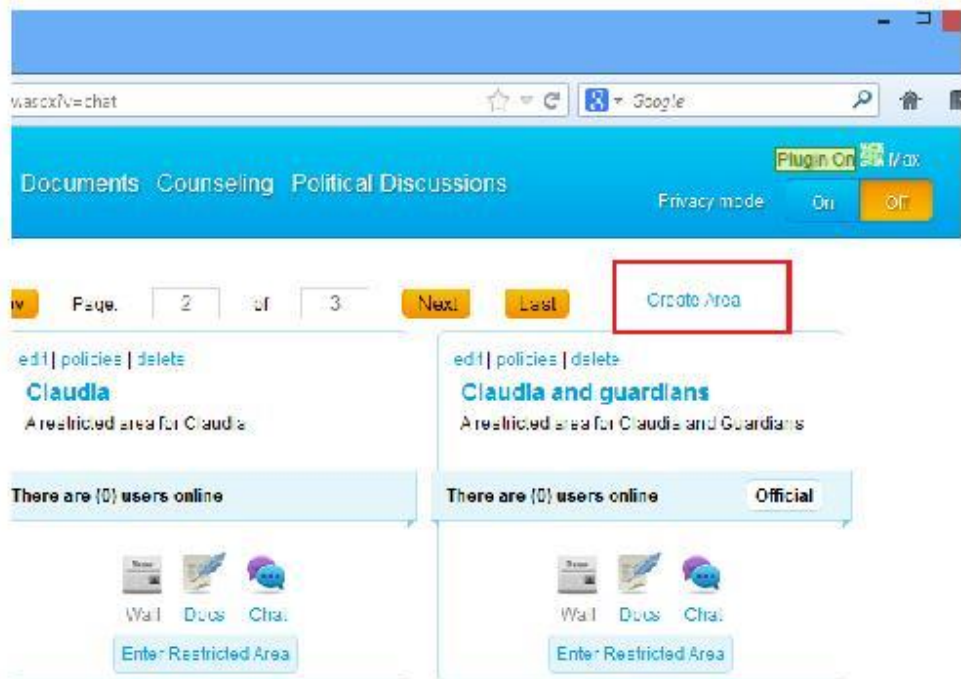


Figure 60 Create Area

ABC4Trust

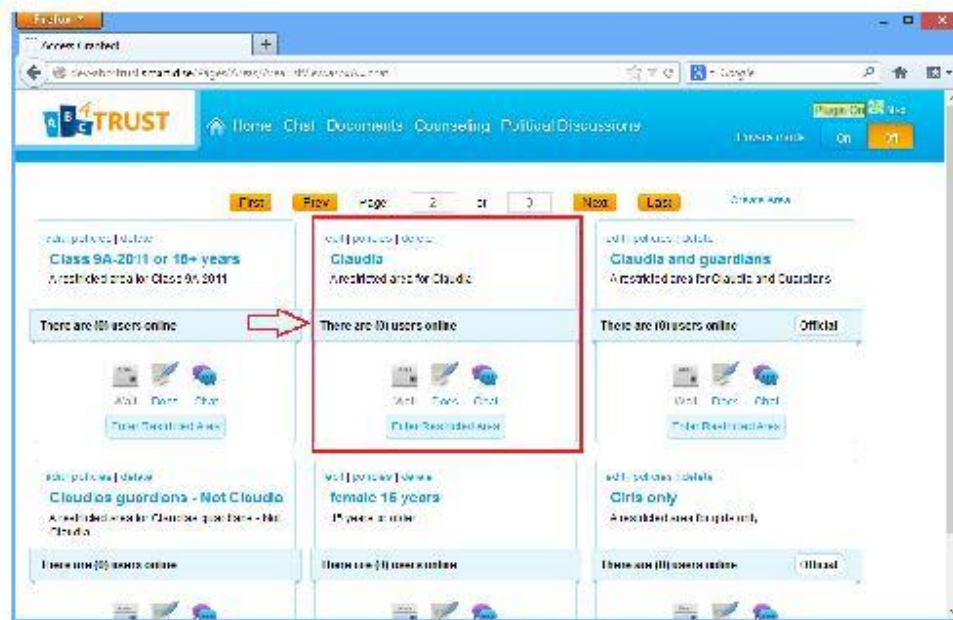


Figure 61 Restricted Area example

ABC4Trust

2.3 How to use Alias Selector

1.1.1 Create new Alias

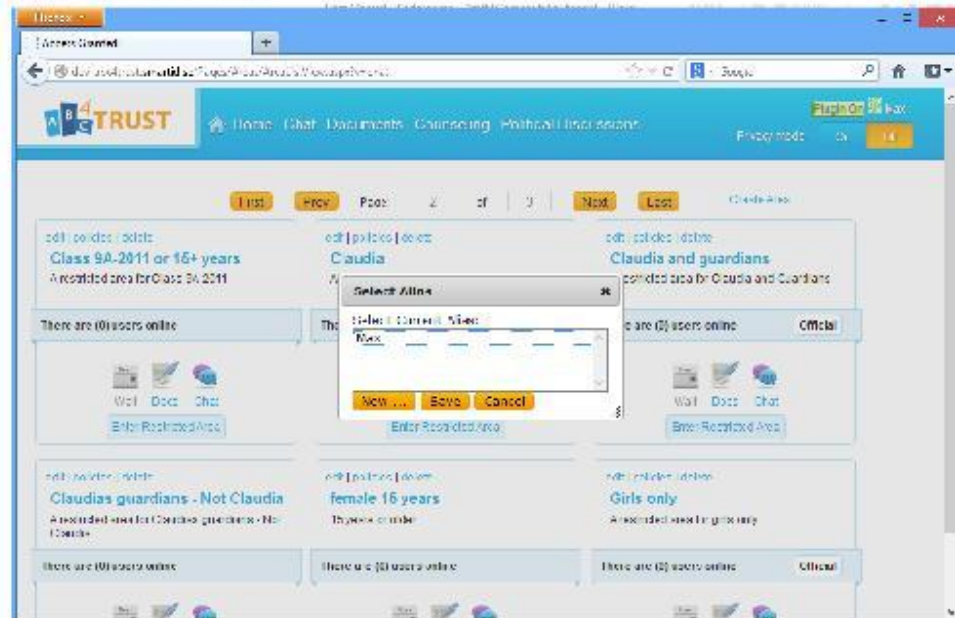


Figure 62 Open Alias Selector

ABC4Trust

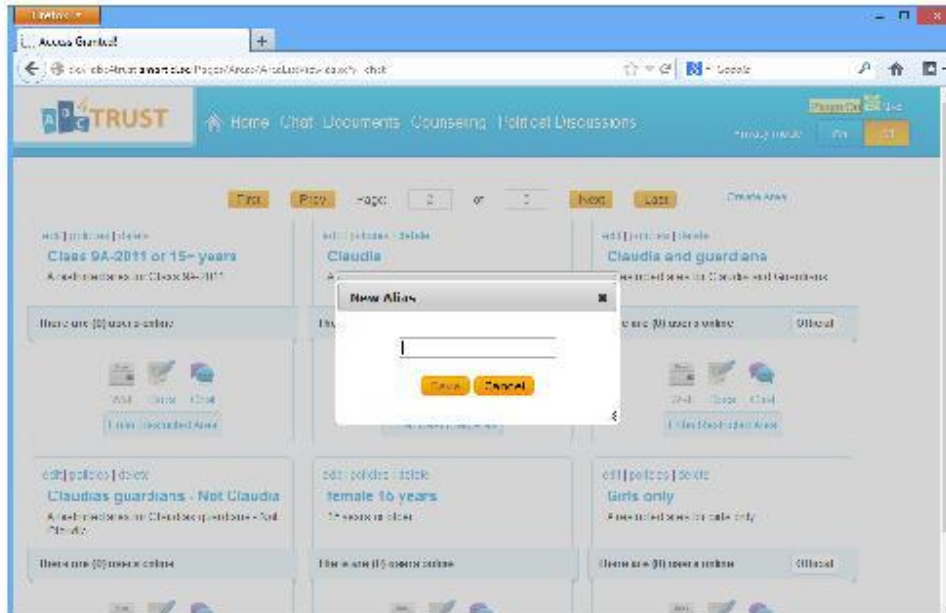


Figure 63 Click "New" to create Alias

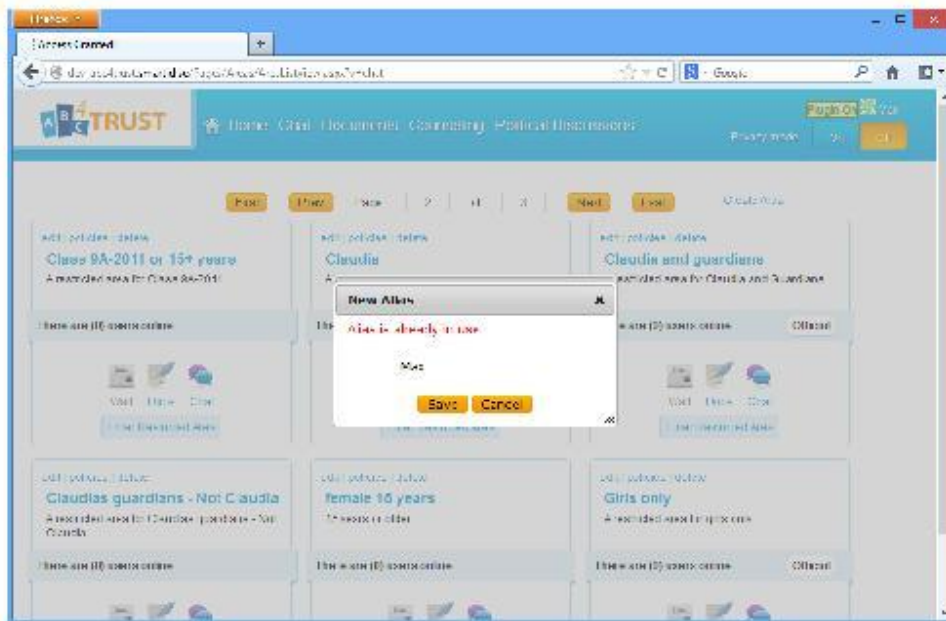


Figure 64 If alias exists, you will get an error

ABC4Trust

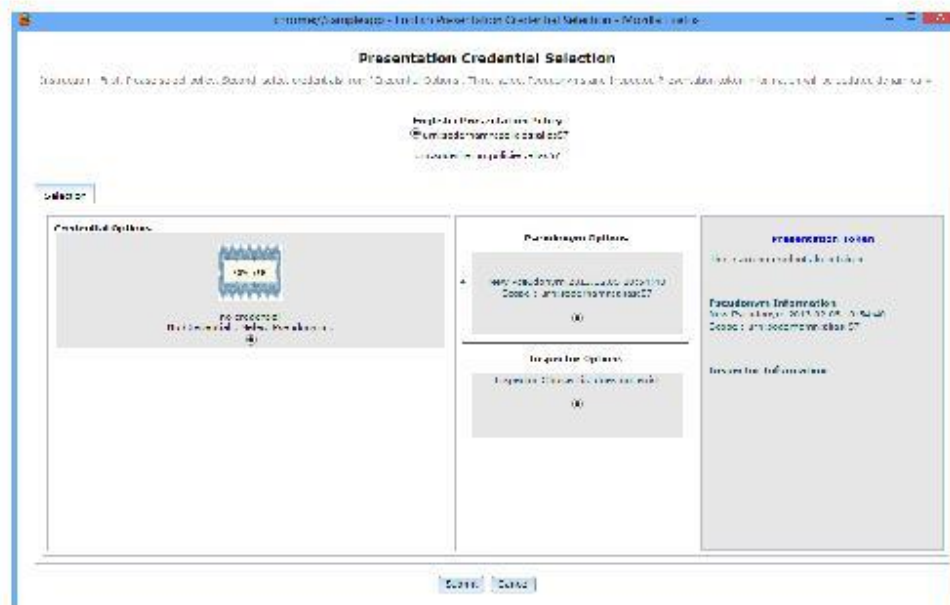


Figure 65 If Alias can be created, Smart Card UI will popup

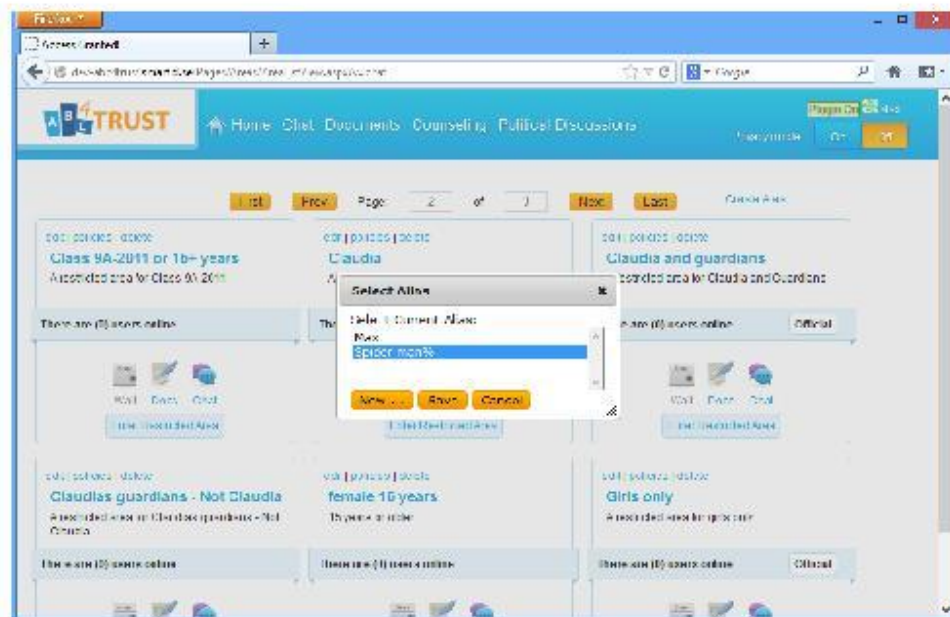


Figure 66 After creation alias will appear in list. Click save to use new Alias, Smart Card UI will popup

ABC4Trust

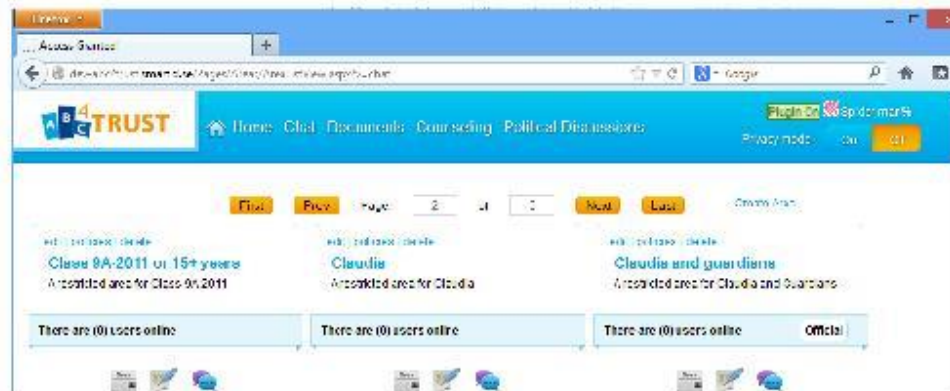


Figure 67 New Alias is at use

1.1.2 Use the Alias

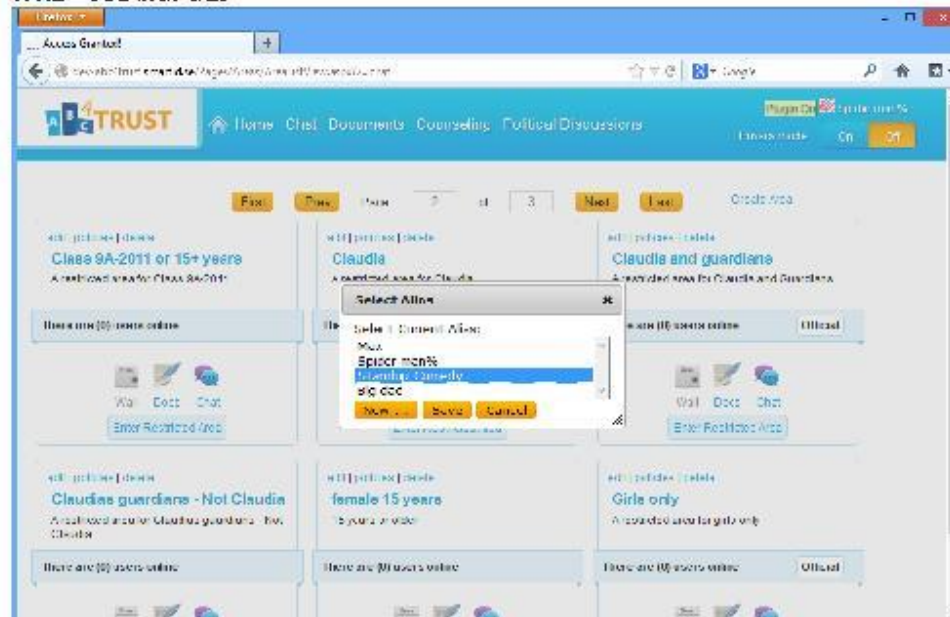


Figure 68 Click on Alias to call Alias Selector

ABC4Trust

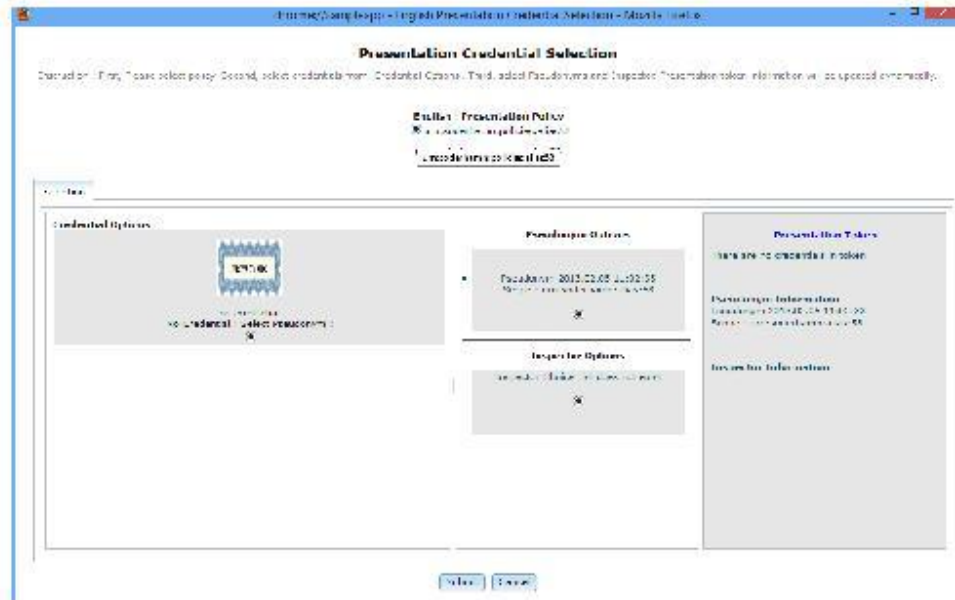


Figure 69 Interact with Smart Card

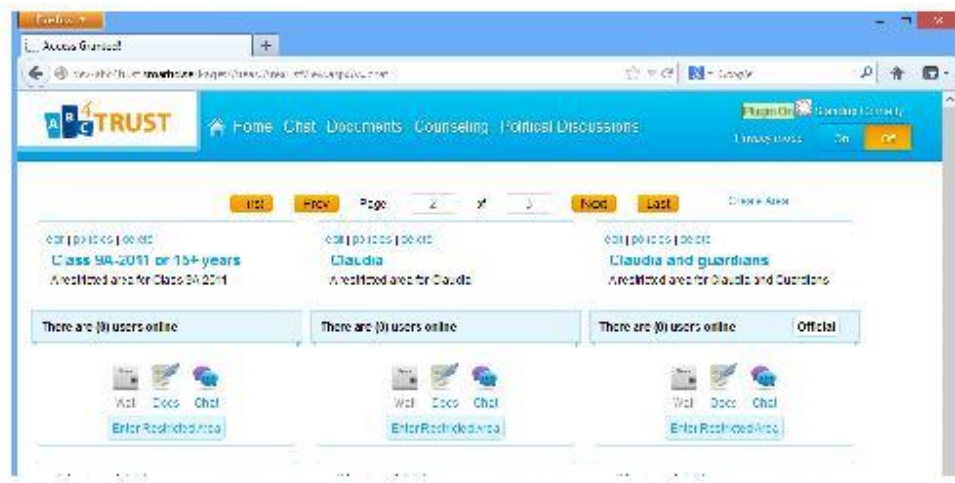


Figure 70 See the Alias at use

2.4 How to use the Dashboard

Dashboard is a part of interface of the School Pilot. It contains Restricted Areas which are:

- **Recently** accessed by one of the aliases of the user

ABC4Trust

- Marked as **favorite** by one of the aliases of the user
- Is a **private Area** for user's primary alias

Click the "Home" link to see the dashboard. During opening dashboard, system will make set of queries to the Smart Card. Please check 1.3 Smart Card User Interface.

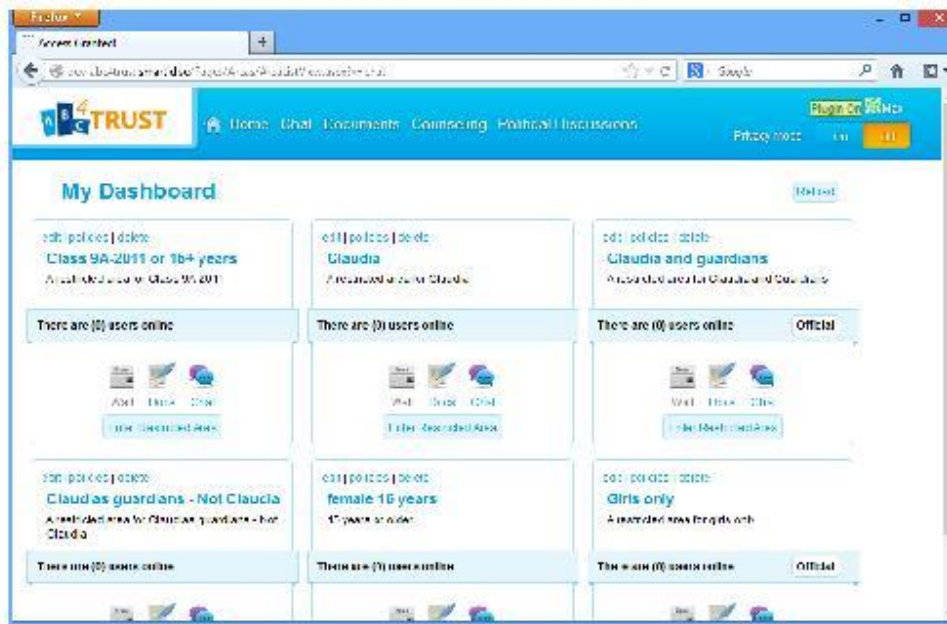


Figure 71 Click on "Home" link to open dashboard

From this window you can do the same actions as from other lists of Restricted Areas:

- Use Alias Selector
- Enter the Restricted Area
- Mark/Unmark Area as favorite
- Query to edit Restricted Area
- Use main menu

2.5 How to Search for and Enter the Restricted Area

User can find Restricted Areas on own Dashboard or under sections of main menu including Political Discussions and Counseling.

ABC4Trust

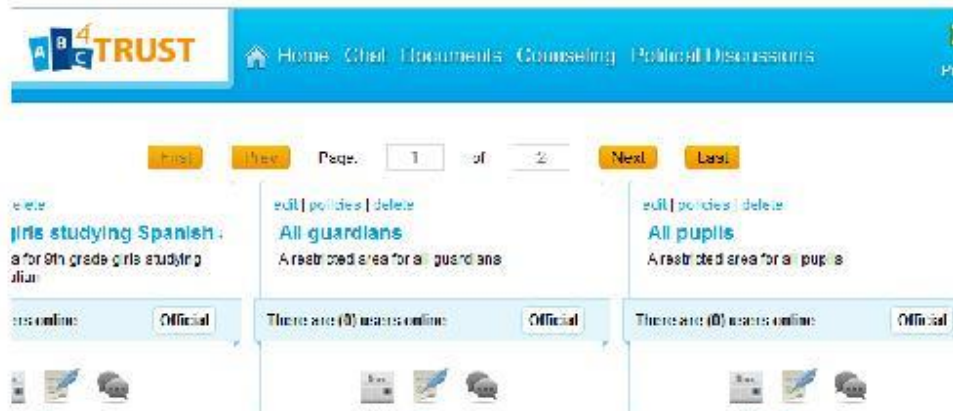


Figure 72 Main menu on top of this image

To enter the Restricted Area user have to hit "Enter Restricted Area" button

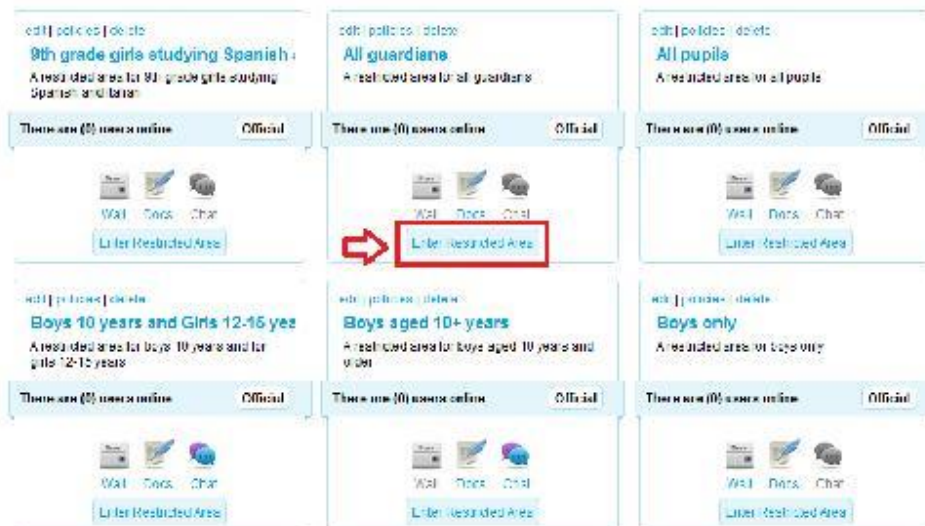


Figure 73 Click "Enter"

New window will be opened with Access Policy details, the same time – Smart Card User Interface popup will appear and request access to verify your credentials.

ABC4Trust



Figure 74 Access Policy Details

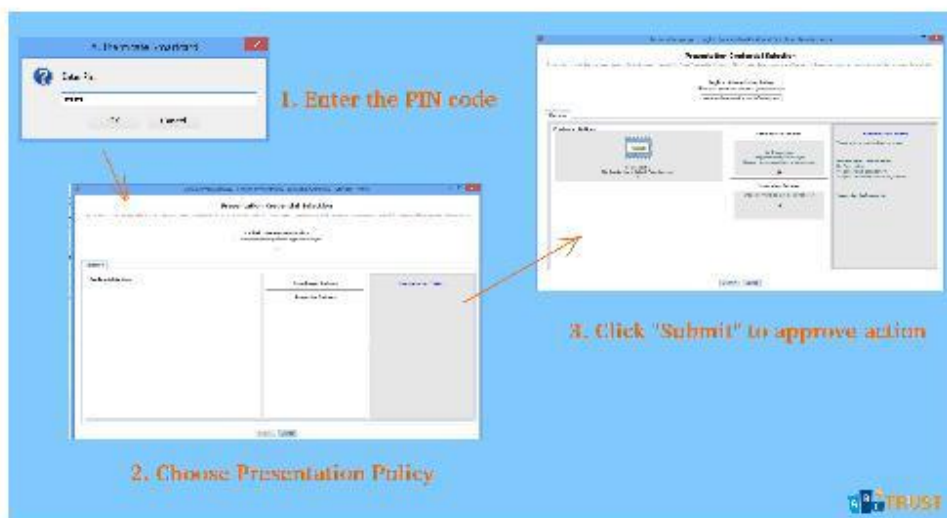


Figure 75 Smart Card Interface described in Chapter 3.3

ABC4Trust



Figure 76 Successfully entered the Restricted Area

2.6 How to use Wall

Wall is a functionality of Restricted Area which allows users to post some important information visible for all Area users.

There's a possibility to "Report Content" to the School Administration if it is violating somebody's rights, more detailed about this in Chapter 3.6 How to use Inspection.

ABC4Trust

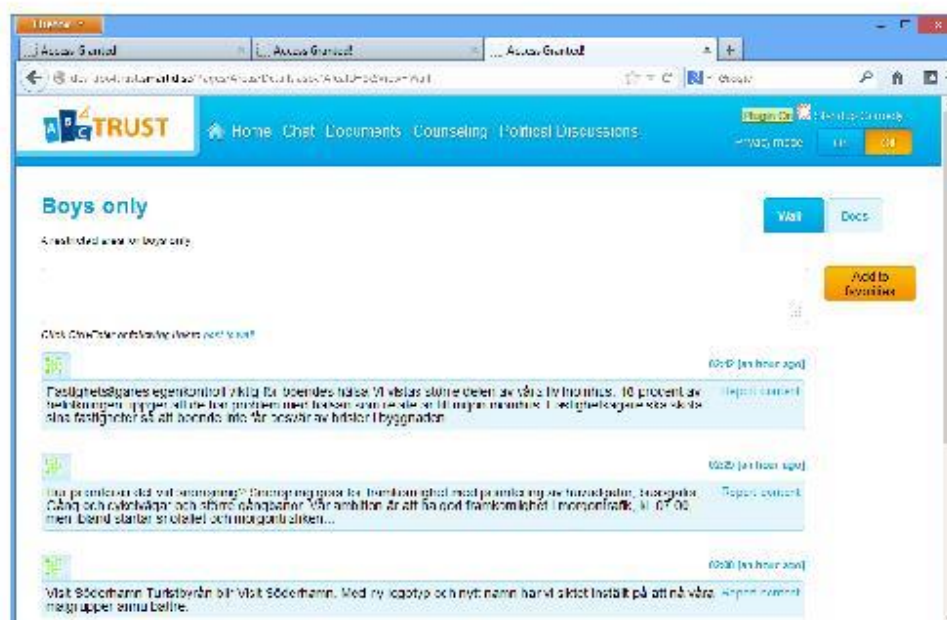


Figure 77 General view on wall

Enter some text to the area and click "Ctrl+Enter" shortcut on keyboard or blue link "post to wall" below the text area

ABC4Trust

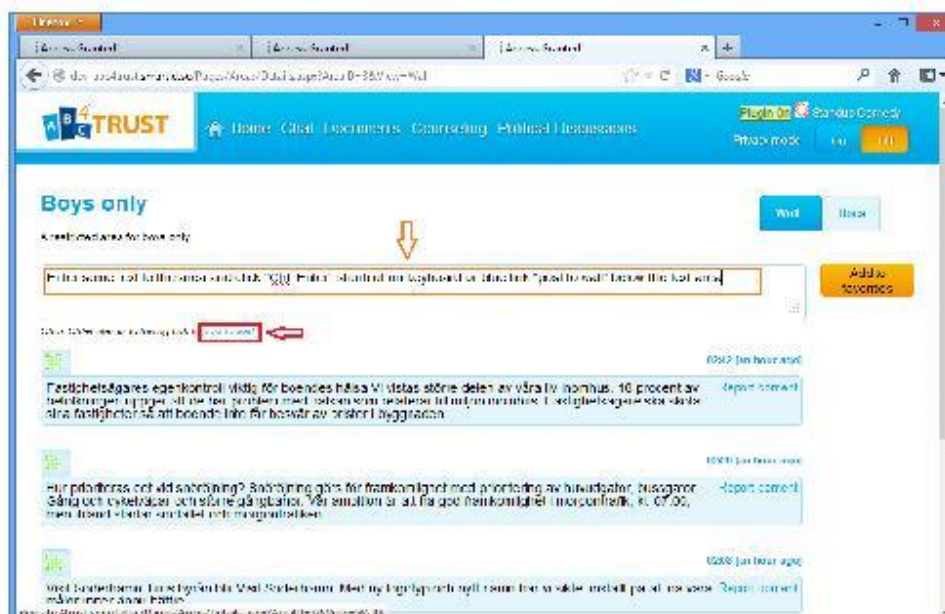


Figure 78 Add content to the wall

The content appears on the wall and is visible to everybody.

2.7 How to use Documents

In documents section users are able to download and upload files to share them within Restricted Area.

To open documents simply click on "Docs" tab of Restricted Area.

You will see the list of available documents and a form to upload new files.

2.8 How to use Chat

Chat is a functionality which is adding possibility for users to have live conversations in Restricted Areas using their aliases.

Users can see last messages sent by themselves and other users, list of online users and a form to enter a new message.

If any of messages is a threat against user – it can be reported to the School Administration. Read more in Chapter 3.6 How to use Inspection.

ABC4Trust

3 Additional Features

3.1 How to Revoke or change Credentials

todo

3.2 How to Backup Your SC's Data

User Smart Card stores all credentials and alias information which is needed to prove its' ownership and use in applications. Alias information is not stored anywhere else, only on user Smart Card. To prevent the case that user might lose the card and access to owned information – ABC4Trust has a feature to backup the Smart Card contents.

Following steps have to be done before you can backup your card:

- You need to have initialized Smart card and credentials on it, according to "How to Register Your Smart Card?" and "How to Obtain All Credentials?"
- You must have installed the ABC4Trust service at your computer
- You have to plug the USB cable of card reader to your computer and place the smart card into the card reader as the "Figure 15 Place Smart Card" shows.

Step 1

Open your web browser. You will see the following interface on your screen. Follow the tab "Tools" at your Firefox browser menu.

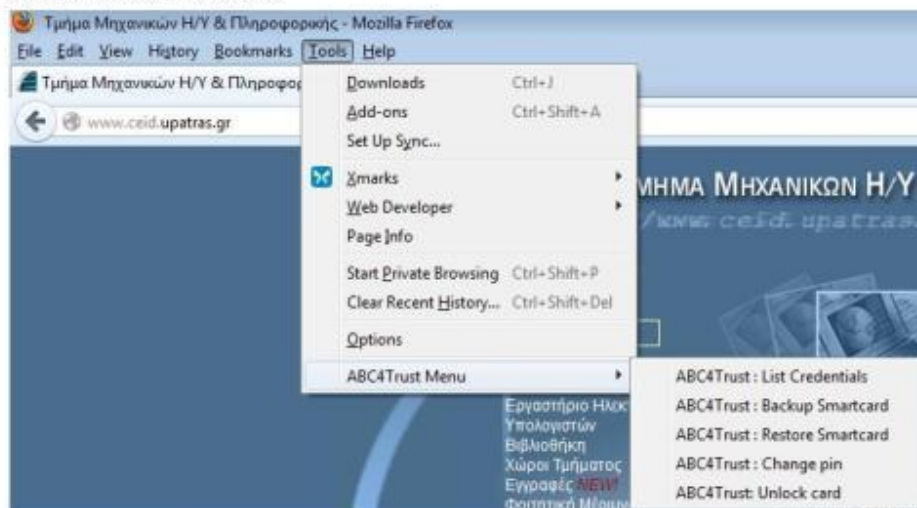


Figure 79 Web Browser menu

ABC4Trust

Step 2

Now select the “ABC4Trust Menu” tab under the Tools Menu as figure below shows.

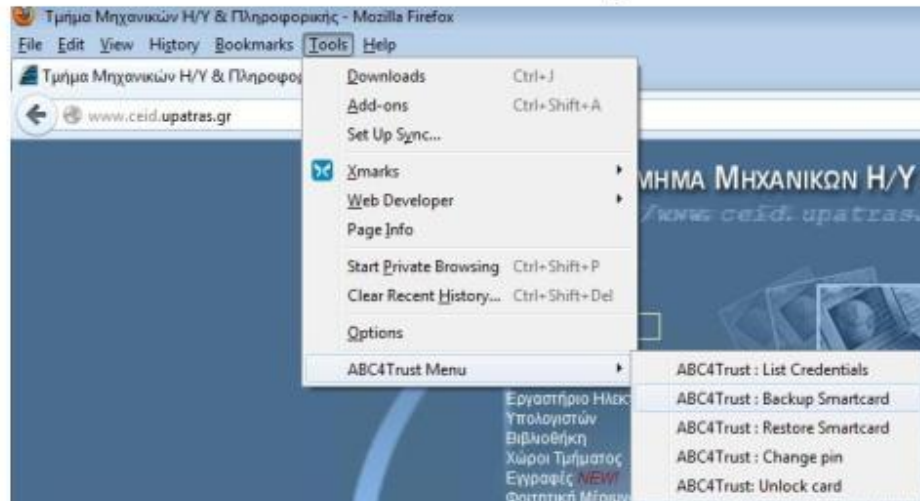


Figure 80 ABC4Trust menu

Step 3

Now please select the “ABC4Trust: Back Up Smartcard” tab under the ABC4Trust. You may receive the following warning message, please select “Continue”.

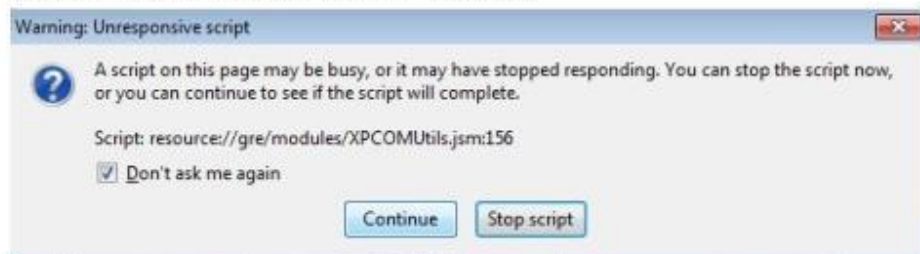


Figure 81 Click "Continue"

Step 4

Now you will receive the following notification message.

ABC4Trust

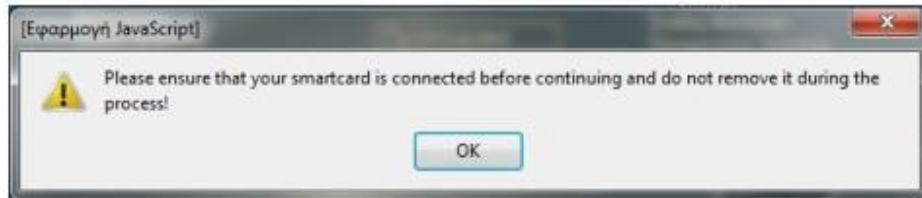


Figure 82 Notification

Step 5

The ABC4Trust User Service application requests your PIN in order to unlock the card. Please enter your PIN in the corresponding box and click the “OK” button.

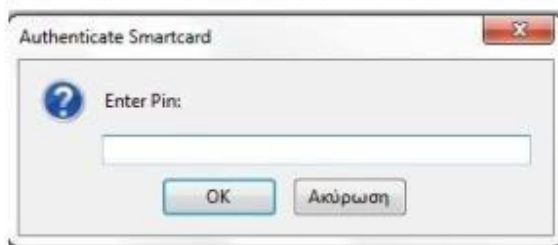


Figure 83 Smart Card PIN entry

Step 6

At this point you have to select a password in order to encrypt your back up information.

Enter your password in the corresponding box as shown the below and click on “OK” button.



Figure 84 Choose password

It is strongly recommended to remember the password, otherwise you will not be able to use a backup.

Step 7

If your SC data has successfully stored at your pc you will see the following message

ABC4Trust



Figure 85 Backup success

Step 8

Your smart card backup file, should now be stored under the directory C:\Program Files\ABC4Trust\User Service\user_storage.

3.3 How to Restore SC's Data

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

Please do not forget about following rules which guarantee your privacy and comfort:

- If you have lost your smart card then you have to declare the smart card loss to the School Administration and to get a new envelope and a new smart card.
- You have a backup on your PC.
- You have to plug the USB cable of card Reader to your computer and place the new smart card into the card reader as it is shown on Figure 15 Place Smart Card.
- You must have installed the ABC4Trust service at your computer.

Step 1

Open your Firefox browser. You will see the following interface on your screen. Follow the tab "Tools" at your Firefox browser menu.

Step 2

Now select the "ABC4Trust Menu" tab under the Tools Menu as figure below shows.

ABC4Trust

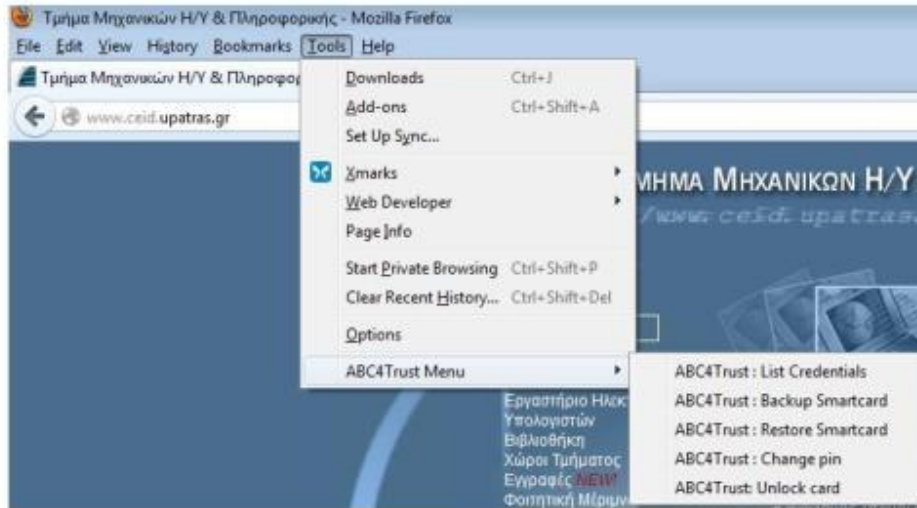


Figure 86 Web Browser menu

Step 3

Now please select the “ABC4Trust: Restore Smartcard” tab under the ABC4Trust Menu

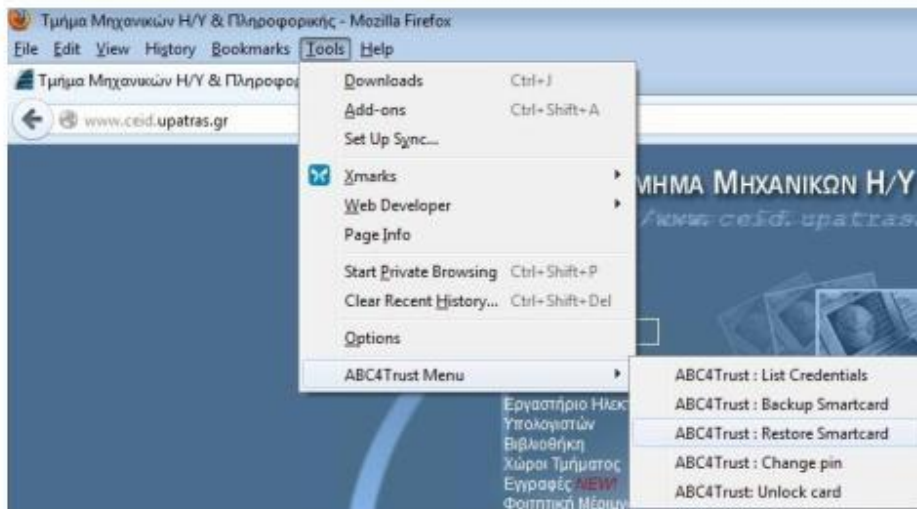


Figure 87 Restore Smart Card

Step 4

ABC4Trust

Now you will receive the following notification message.

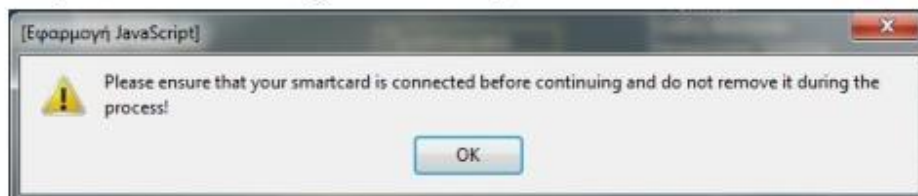


Figure 88 Notification

Step 5

The ABC4Trust User Service application requests your PIN in order to unlock the card. Please enter your PIN in the corresponding box and click the “OK” button.

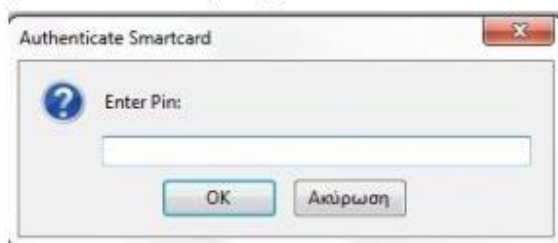


Figure 89 Check the PIN

Step 6

At this point you have to enter your password (that you selected at step 6 see Section 3.7) in order to decrypt your back up information.

Enter your password in the corresponding box as shown the below and click on “OK” button.



Figure 90 Enter the password from backup

Step 7

ABC4Trust

If your stored data has successfully restored at your smart card you will see the following message



Figure 91 Success message

Step 8

Finally, please restart your computer in order for the ABC4Trust User Service to be restarted.

3.4 How to Change Your PIN

Every user of the School Pilot is able to change the PIN code for a Smart Card. It's strictly recommended to change the PIN in case you think or know that somebody might know it.

To start the procedure please make sure that following as done:

- You have installed the ABC4Trust service at your computer.
- You have to plug the USB cable of card reader to your computer and place the smart card into the card reader as the Figure 15 Place Smart Card shows.

Step 1

Open your Firefox browser. You will see the following interface on your screen. Follow the tab "Tools" at your Firefox browser menu.

Step 2

Now select the "ABC4Trust Menu" tab under the Tools Menu as figure below shows.

ABC4Trust

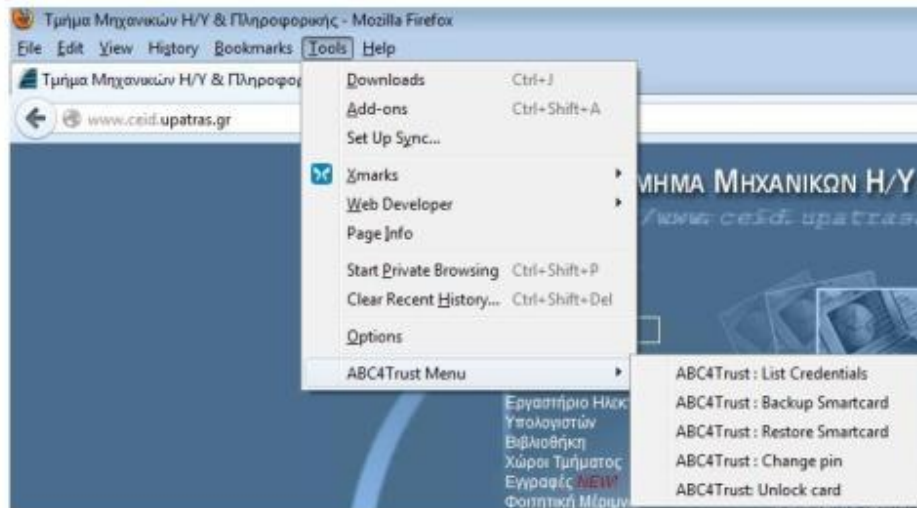


Figure 92 Web Browser menu

Step 3

Now please select the “ABC4Trust: Change pin” tab under the ABC4Trust Menu

Step 4

Now you will receive the following notification message.



Figure 93 Notification

Step 5

The ABC4Trust User Service application requests your current PIN in order to unlock the card. Please enter your current PIN in the corresponding box and click the “OK” button.

ABC4Trust



Figure 94 Enter PIN

Step 6

Now, please enter your new PIN in the corresponding box and click the "OK" button.



Figure 95 Enter new PIN

Step 7

If your PIN has been successfully changed you will see the following message and select "OK".

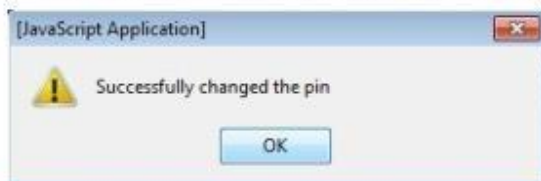


Figure 96 Success message

ABC4Trust

3.5 How to Unlock Your Smart Card

If the user enter the PIN to the Smart Card wrong three times –the card get locked to prevent somebody picking up your PIN and use the card instead of user.

If the PIN was entered wrong just by mistake, user has an ability to unlock the card.

To start the procedure please make sure that following as done:

- You have installed the ABC4Trust service at your computer.
- You have to plug the USB cable of card reader to your computer and place the smart card into the card reader as the Figure 15 Place Smart Card shows.

Step 1

Open your Firefox browser. You will see the following interface on your screen. Follow the tab “Tools” at your Firefox browser menu.

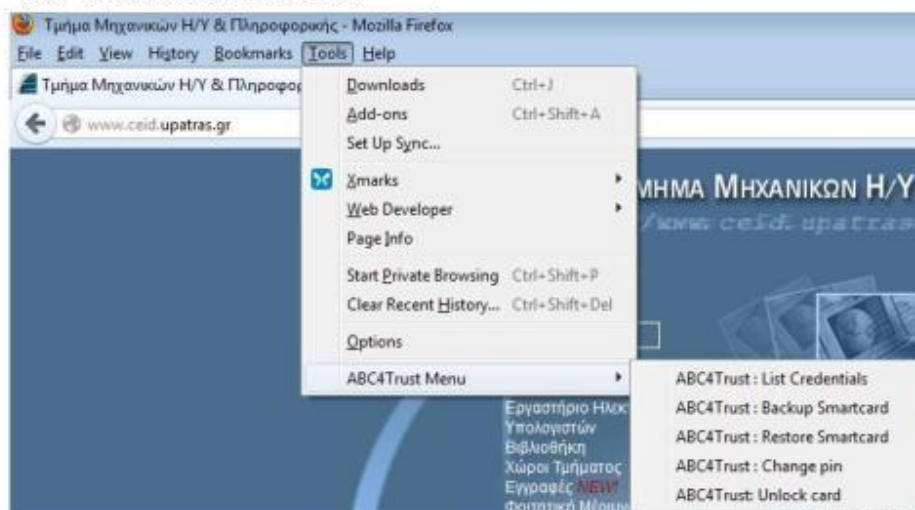


Figure 97 Web Browser menu

Step 2

Now select the “ABC4Trust Menu” tab under the Tools Menu and choose item “Unlock card” as shown below

ABC4Trust

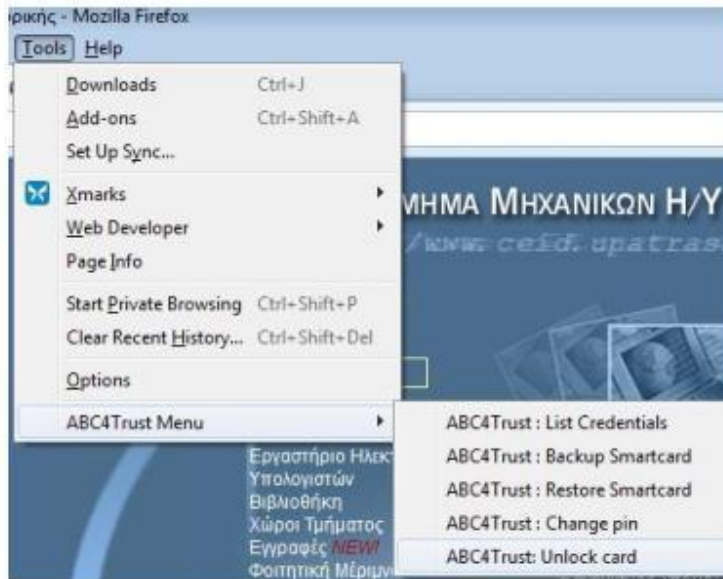


Figure 98 Choose Unlock card

Step 3

Now you will receive the following notification message.



Figure 99 Notification message

Step 4

The ABC4Trust User Service application requests your PUK. Please enter your PUK (it is included in the sealed envelope see Figure 3. PIN and PUK from letter) in the corresponding box and click the "OK" button.

ABC4Trust



Figure 100 Enter PUK

Step 5

Now, please enter your new PIN in the corresponding box and click the "OK" button.



Figure 101 Enter new PIN

Step 6

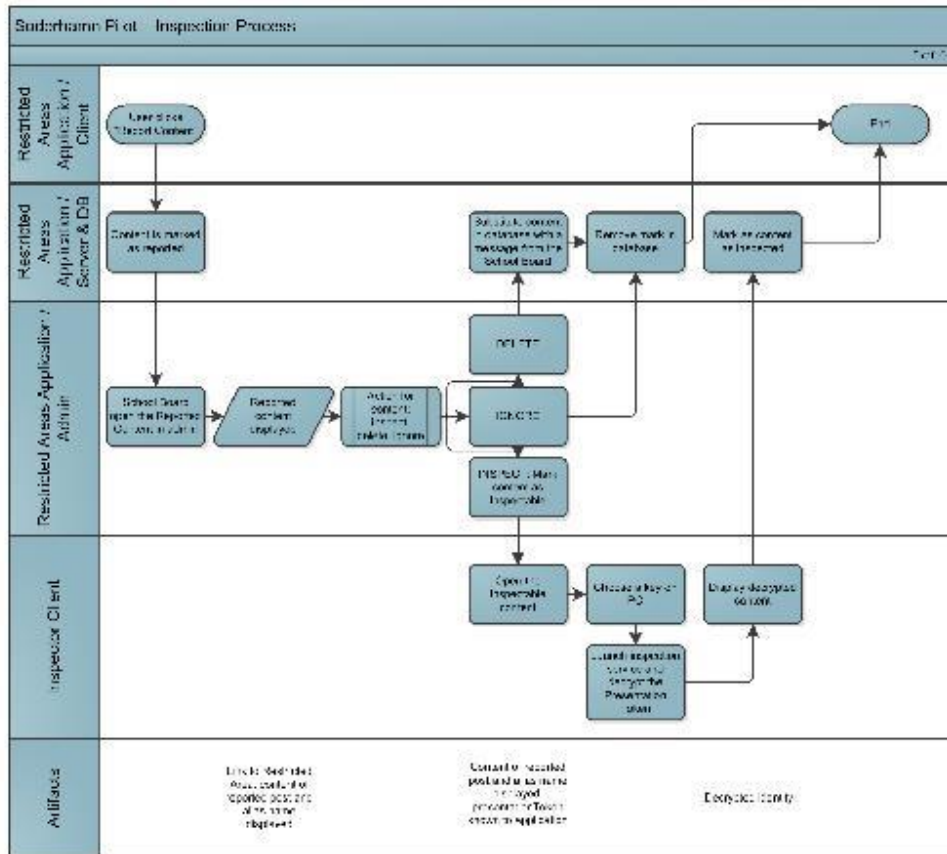
If your Smart Card unlocked successfully and you will see the following message and select "OK".



Figure 102 New PIN was chosen

ABC4Trust

3.6 How to use Inspection



ABC4Trust

4 Contacts

In case if you need more support or have problems using the software, please **contact...**

Glossary

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).

In the Swedish School Pilot the following attributes were used: *firstname, lastname, birthdate (age), gender, class, school name, roles, subjects, children and guardians*. The attribute guardian (issued to pupils) indicates a pupil's guardians. And the attribute child (issued to guardians) indicates the children of a guardian.

Access Policy

An access policy indicates who is allowed to enter and to use the functionality (read/write messages, upload/download documents etc.) of a Restricted Area. The XML Each Restricted Area has its own access policy stating who is entitled to access/enter a Restricted Area e.g. a 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 older than 12 years
- Only for class 7A
- Claudia Hugosson
- Teachers

Access policies are translated into the XML style presentation policy alternatives via the XML Generator in the RA Application.

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.

Certified pseudonym

A verifiable pseudonym based on a device 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 device 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.

In the Swedish School Pilot the following credentials are used: *credSchool, credSubject, credChild, credGuardian and credRole*.

Credential specification

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

Key binding

An optional credential feature whereby the credential is bound to a strong secret so that any presentation token involving the credential requires the presence of the key.

IdM Database

The Identity Management Database is a database where all User data (attributes) needed to issue credentials are saved.

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 Board

In the Swedish Pilot the inspection board consists of three persons that in emergency situations will investigate if the inspection grounds are met. The inspection board will decide whether an inspection can take place or not. The decision is forwarded to the inspector who has the inspector key needed to perform an inspection.

Inspection grounds

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

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.

In the Swedish School Pilot the school is the Issuer.

Issuer parameters

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

Linkability

See *unlinkability*.

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 policy alternatives

A choice/list for presentation policies.

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, key binding, inspection, and revocation. The presentation token consists of the presentation token description, containing a technologies-agnostic description of the revealed information, and the presentation token evidence, containing opaque technologies-specific cryptographic parameters in support of the token.

Privacy-ABC

A common name to describe privacy friendly technologies developed within the ABC4Trust project.

Pseudonym

See *verifiable pseudonym*.

Pseudonym scope

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

Restricted Area

See *restricted area application*.

Restricted Area Application

The restricted Area Application is the school web application that contains all the functionality for chat, wall, documents uploading, counseling and political discussions. The restricted Area Application is also an tool that offers functionality to create, delete and update different Restricted Areas. Each Restricted Area is protected by one or several Access Policies indicating who is allowed to enter and access the content within the RA.

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. 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.

Pilot User Number

Pilot User Number (PUN) is a number (10 digits) used in the pilot to uniquely identify the Users. The PUN consists of the birthdate of the User and a number (980112-XXXX). The PUN used in the pilot is not the same as the Swedish Civic Registration Number.

Scope

See *pseudonym scope*.

Scope-exclusive pseudonym

A certified pseudonym that is guaranteed to be cryptographically unique per scope string and per device secret. Meaning, from a single device bound key, 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.

The Users in the Swedish School Pilot are pupils, guardians and school personnel.

The Users in the Patras Pilot are students.

User agent

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

Device binding

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

Device secret

A piece of secret information known to a device (a strong random secret) underlying one or more issued credentials or pseudonyms. A presentation token involving a pseudonym or a device-bound credential implicitly proves knowledge of the underlying secret.

Verifiable pseudonym

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

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.

List of Acronyms

ABCs	Attribute Based Credentials
ABCE	ABC Engine
Admin	Short form of ‘administrator’
CA	Certificate Authority
FP7	Framework Programme 7
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technologies
ID	Identifier
Idemix	IBM Identity Mixer
IdM	Identity Manager
ISO	International Organisation for Standardisation
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
Privacy-ABCs	Privacy Attribute Based Credentials (privacy ABCs)
PUK	Personal Unblocking Key
PUN	Pilot User Number
RA	Restricted Area
RevAuth	Revocation Authority
SC	Smart Card
SCI	Smart Card Interface
URL	Uniform Resource Locator
WP	Work Package
XML	Extensible Markup Language

7 Bibliography

- [BGL+12] Souheil Bcheri, Norbert Götze, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Yannis Stamatiou, Katalin Storf, Peder Wängmark, Harald Zwingelberg, “D5.1 Scenario Definition for both Pilots”, 2012
- [D53] Souheil Bcheri, Kasper L. Damgård, Daniel Deibler, Norbert Götze, Hans G. Knudsen, Maksym Moneta, Apostolos Pyrgelis, Eva Schlehahn, Michael B. Stausholm, Harald Zwingelberg, “D5.3 Experiences and Feedback of the Pilots”, 2014
- [D61] Souheil Bcheri, Norbert Goetze, Monika Orski, Harald Zwingelberg, “D6.1 Application Description for the school deployment”, 2014
- [D62] Joerg Abendroth, Souheil Bcheri, Kasper Damgaard, Hamza Ghani, Jesus Luna, Gert Læssøe Mikkelsen, Maxim Moneta, Monika Orski, Neeraj Suri, Harald Zwingelberg, “D6.2 Necessary hardware and software package for the school pilot deployment”, 2014
- [D71] Joerg Abendroth, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Ahmad Sabouri, Eva Schlehahn, Yannis Stamatiou, Harald Zwingelberg, “D7.1 Application Description for students”, 2014
- [D73] Daniel Deibler, Malte Engeler, Ioannis Krontiris, Vasiliki Liagkou, Apostolos Pyrgelis, Eva Schlehahn, Yannis Stamatiou, Welderufael Tesfay, Harald Zwingelberg, “D7.3 Evaluation of the Student Pilot”, 2013