Integrating and trialling Attribute-based Credentials on Smartcards for building trust
The ABC4Trust project

Ahmad Sabouri, Jonas Lindstrøm Jensen, Kasper Lyneborg Damgård, Janus Dam Nielsen, Kai Rannenberg[1]

Abstract

Along with the convenience that came with the penetration of electronic transactions and services into our everyday life, new security and privacy threats have been emerging. The necessity of employing privacy-preserving technologies in order to avoid online surveillance is getting more and more attention. In this regard, the EU project ABC4Trust[2] has been the pioneer to deploy the first ever trial of Privacy Preserving Attribute-based Credentials (Privacy-ABCs) in real life environment. In this paper, we provide an overview of the state of ABC4Trust's work in the design and development of the ABC4Trust architecture as well as the integration of smartcards into the deployed pilots.

1 Introduction

The rapid growth of communication infrastructures and enterprise software solutions has caused electronic services to penetrate into our everyday life. So it is not far from reality that many personal and trust-sensitive transactions happen online. In this regard, one of the biggest challenges to deal with will be proper user authentication and access control, as strong authentication and authorization techniques used nowadays are double-edged swords: while they can protect service providers by offering a satisfactory level of resilience against unauthorized accesses, most of these technologies have the drawback of threatening the clients' privacy.

As an example, X.509 certificates, which are one of the most common strong authentication mechanisms, contain a list of attributes of users attested and digitally signed by a trusted issuer in the domain. The static representation of these certificates makes it possible to trace users' online activities and link their various transactions. Furthermore, due to the nature of these certificates, the signature cannot be verified if a single modification occurs in the issued certificates. As a result, there is no choice for the users other than revealing all the attested attributes in their transactions even though some of them are not needed. Online techniques like SAML, OpenID, or WS-Federation can overcome this problem and offer selective disclosure of attributes, but they still suffer from other privacy breaches.

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

[2] https://abc4trust.eu

Taking OpenID as an example, the OpenID Provider is actively involved in the authentication process. This means the users cannot access a service without the OpenID Provider learning about that transaction. Therefore, the OpenID Provider knows about every authentication session and it can profile the users based on their requested services. On the other hand, when a service provider employs OpenID to authenticate its users, the OpenID Provider can monitor the service provider's business as well and build a profile based on the number of authentication requests and the information it has about the requesting users. In addition to these privacy threats for users and service providers, there is a risk of impersonation of the user by the OpenID Provider, since the user does not have an active involvement in the information exchange process between the OpenID Provider and the service provider.

This paper provides an overview of ABC4Trust's results so far in deploying trials for privacy enhancing technologies and integrating smartcards into the pilots. We start with a brief introduction of Privacy Preserving Attribute-based Credentials (Privacy-ABCs) and their life-cycle in Section 2. Then in Section 3, we present the proposed architecture by ABC4Trust for Privacy-ABC systems. Section 4 describes the trials where ABC4Trust brings Privacy-ABCs into practice. In Section 5, we shortly talk about the Reference Implementation of the proposed architecture, and later elaborate on the integration of smartcards into our scenarios in Section 6. We conclude the paper with an outlook in Section 7.

2 Privacy Attribute-based Credentials

Privacy Preserving Attribute-based Credentials (Privacy-ABCs) are elegant techniques to cope with the problems we introduced in the previous section. They can offer strong authentication and a high level of security to service providers, while users' privacy is preserved, so the follow the paradigm of Multilateral Security [Rann00]. Users can obtain certified attributes in the form of Privacy-ABCs, and later derive unlinkable tokens that only reveal the necessary subset of information needed by the service providers.

Over the past years, there have been several proposals on how to realize a Privacy-ABC system [Chau85, Bran93, CaLy01, CaLy04]. However, there was no commonly agreed set of functions, features, formats, protocols, and metrics to gauge and compare these Privacy-ABC technologies, and it is hard to judge the pros and cons of the different technologies to understand which ones are best suited to which scenarios [CKL+11]. ABC4Trust provides definitions of Privacy-ABCs' concepts such as pseudonyms, credentials, (key-) binding and the processes of issuance, presentation, revocation and inspection, presenting a complete overview of the life-cycle of Privacy-ABCs.

A **Credential** is defined to be "a certified container of attributes issued by an **Issuer** to a **User**" [CKL+11]. An Issuer vouches for the correctness of the attribute values for a User when issuing a credential for her. For example, a university can issue an "Enrolment Credential" for a student, which contains several attested attributes such as firstname, lastname, matriculation number and the enrolment year.

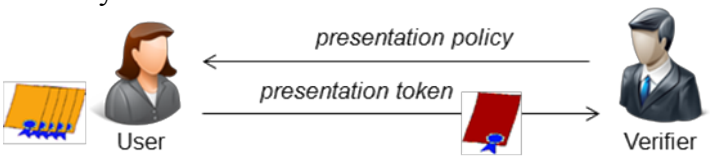

Figure 1: A Sample Presentation Scenario

A typical authentication scenario using Privacy-ABCs is shown in Figure 1, where a User seeks to access an online service offered by a Service Provider. The Service Provider performs a so-called Verifier role and expresses its requirement for granting access to the service in form of a **Presentation Policy**. In the next step, the User needs to come up with a combination of its credentials to derive an acceptable authentication token that satisfies the given policy. When the Verifier confirms the authenticity and credibility of the **Presentation Token**, the User gets access to the corresponding service.

Presentation tokens based on Privacy-ABCs are cryptographically proven to be unlinkable and untraceable, meaning that Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials, and that Issuers cannot trace a presentation token back to the issuance of the underlying credentials. Furthermore, since the User is actively involved into the generation of Presentation Tokens, there is no risk of user impersonation introduced by the other parties.

After this brief introduction of Privacy-ABC scenarios, we quote a more detailed description of the involved entities in the life cycle of Privacy-ABCs and demonstrate in Figure 2 their interactions as Deliverable 2.1 of ABC4Trust [CKL+11] presents them:

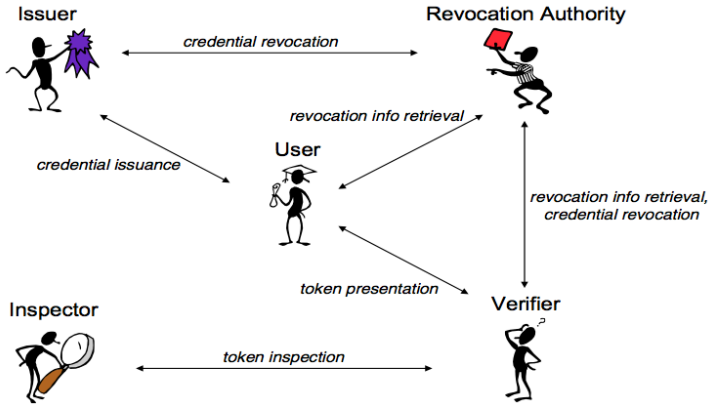

Figure 2: Privacy-ABCs' entities and their interactions [CKL+11]

- "The **User** is at the centre of the picture, collecting credentials from various Issuers and controlling which information from which credentials she presents to which verifiers. The human User is represented by her User Agent, a software component running either on a local device (e.g. on the User's computer or mobile phone) or remotely on a trusted cloud service. The User may own special hardware tokens to which credentials can be bound to improve security. In identity management literature, the User is sometimes referred to as the requestor or the subject.
- An **Issuer** issues credentials to Users, thereby vouching for the correctness of the information contained in the credential with respect to the User to whom the credential is issued. Before issuing a credential, the Issuer may have to authenticate the User, which it may do using Privacy-ABCs, using a different online mechanism (e.g., username and password), or using out-of-band communication (e.g., by requiring the User to physically present herself at the Issuer's office). In the identity management literature, the Issuer is sometimes referred to as the identity provider or attributes authority.

- A **Verifier** protects access to a resource or service that it offers by imposing restrictions on the credentials that Users must own and the information from these credentials that Users must present in order to access the service. The Verifier's restrictions are described in its presentation policy. The User generates from her credentials a presentation token that contains the required information and the supporting cryptographic evidence. In the identity management literature, the Verifier is sometimes also referred to as the relying party, the server, or the service provider.
- A **Revocation Authority** is responsible for revoking issued credentials, so that these credentials can no longer be used to generate a presentation token. Both the User and the Verifier must obtain the most recent revocation information from the Revocation Authority to generate, respectively verify, presentation tokens.
- An **Inspector** is a trusted authority who can de-anonymize presentation tokens under specific (and extreme) circumstances. To make use of this feature, the Verifier must a-priori specify in the presentation policy, which Inspector should be able to recover which attribute(s) under which circumstances. The User is therefore aware of the de-anonymization options when the token is generated and actively participates to make this possible; therefore the User can make a conscious decision based on her trust in the Inspector."

3 The ABC4Trust Architecture

The architecture has been designed to decompose future (reference) implementations of Privacy-ABC technologies into sets of modules and specify the abstract functionality of these components in such a way that they are independent from the cryptographic mechanisms used underneath. As a result, application developers can integrate the reference implementation of the ABC4Trust architecture directly into their applications, without having to know how its layers are internally structured (Section 5). The functional decomposition foresees possible architectural extensions to additional functional modules that may be desirable and feasible using future Privacy-ABC technologies or extensions of existing ones [CKL+11].

Figure 4 depicts a cropped view of the high level ABC4Trust architecture where two of the main actors, namely User and Verifier, interact in a typical service request scenario. As demonstrated in this figure, the ABC4Trust architectural modules are divided into the three abstract layers, namely Application, ABC-Engine (ABCE) and CryptoEngine (CE). The core of the architecture is the ABCE; it provides the necessary APIs to the application layer residing on the top and utilizes the interfaces offered by the CE that constitutes the bottom layer.

To complete the picture an XML-based language framework has been designed so that ABCE peers from different entities of the system, e.g. the User and the Verifier, can communicate in a technology-agnostic manner. Putting all the pieces together, the application layer follows the corresponding steps defined in the protocol specification [CKL+11], calls the appropriate ABCE APIs, and exchanges the given messages with the other parties. Further down in the layers, upon receiving an API call, the ABCE performs technology-agnostic operations, such as matching the given access policy with the user's credentials, interacting with the user in case it is needed, and invoking crypto APIs from the CE in order to accomplish cryptographic operations. Finally the bottom layer CE is where the different realizations of Privacy-ABC technologies appear and provide their implementations for the required features.

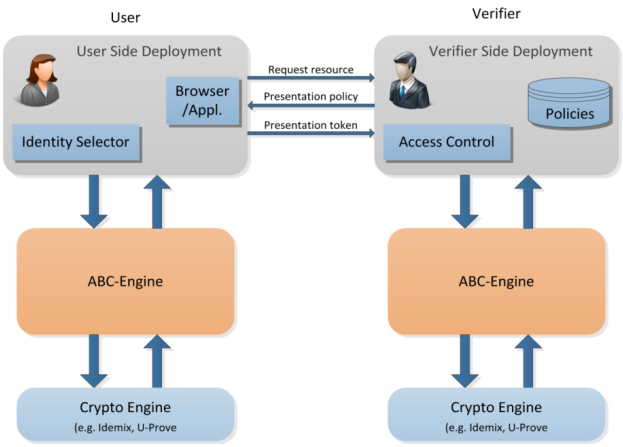

Figure 3: ABC4Trust layered architecture [SaKR12]

Going one level deeper in the architecture components, ABC4Trust has designed a new crypto architecture that breaks down the monolithic implementation of CryptoEngines. This architecture decomposes the crypto realization of Privacy-ABCs into a set of building blocks (i.e. signature schemes, range proofs, etc.) and defines the APIs and interfaces between them. As a result one can customize the CE based on the desired features. Furthermore, the new design facilitates co-existence and interoperability of different Privacy-ABCs as it is the case in the second round of ABC4Trust Course Evaluation pilot, where students use Idemix and U-Prove credentials together in one single presentation.

4 The ABC4Trust Pilots

4.1 Online Course Evaluation

A standard practice at the end of each semester in most universities is to collect the opinions of the students who have taken a course and to evaluate different aspects of that course to further improve the quality of education in the future. However, both the students and the professors have legitimate concerns about the process of course evaluation. The students might be worried about their identities being linked to their evaluation forms, and thus resulting in negative impacts on their grades or education records. On the other hand, professors consider a minimum level of participation in the lectures to be necessary for getting the real experience of the course and therefore being eligible to evaluate it. The scenario becomes even more complex in terms of security, privacy, and trust, when electronic evaluation is desired.

In September 2012, ABC4Trust launched its first pilot in the Patras University in Greece focusing on the online course evaluation process. In the designed scenarios Privacy-ABCs were employed to address the aforementioned concerns of the both parties. Whilst the identity and privacy of the students were being protected, the opinions of the students, who had attended more than a certain number of lectures, were collected via the online evaluation portal.

At the beginning of the semester, the pilot participants received a start-up kit containing a smartcard and its PIN (and PUK) code, a smartcard reader, and a One-Time Password (OTP) to access the Identity Management System (IdM). In the first step, they had to visit the IdM and login with their student ID and their OTP, and then register their smartcards with their profiles. When the card was registered, they could authenticate to the IdM using only the

smartcard. In the next step, they had to download credentials that certify their enrolment in the university and the course.

After the initialization actions were performed at the beginning of the semester, the students could record their participation in the lectures on their smartcards. Upon entering the lecture room, every student had to swipe her card in front of the device installed in the room in order to collect attendance units for that specific lecture. It is important to mention that these units were collected anonymously, meaning that no identifiable information was transferred to the system, which otherwise might have lead to privacy breaches. Therefore, the attendance records were only stored on the smartcards of the students and not anywhere else.

During the evaluation period, the student could access the evaluation form and submit their opinion if they could prove that 1) they are a student of the university, 2) they are registered in the course 3) they have attended at least a minimum number of the lectures from the course. If all these conditions were met, the smartcard could produce a Privacy-ABCs presentation proof that attested their eligibility to evaluate the course. While it was not possible to link the evaluations to the actual participants, the authentication step was designed based on so-called "scope-exclusive pseudonyms", which gives the opportunity to recognize a returning user and therefore allow her to update her previous submission. By the end of this round of the trial in February 2013, 48 students submitted their feedback about the course using the pilot platform.

A second round of the same pilot was launched in Fall 2013 with 60 participants to further test the Privacy-ABC features developed in ABC4Trust in an actual deployment environment. The newly introduced features include revocation of credentials, blind transfer of attributes between credentials and inspection of tokens (de-anonymization). The scenarios of the first round of this pilot were extended in order to best integrate these new features. More specifically, after the students submit their evaluations, they will receive a new credential that has the student ID blindly transferred to it from the university registration credential in their cards. In other words, they get a certificate of participation in the evaluation bound to them without the system being able to identify the students in the corresponding session. They can later use the new credential to anonymously take part in a tombola. When the winner is selected, her identity will be revealed through the inspection of her token. There is no privacy risk for the winner with regard to the evaluation she provided, as the only information one can learn is that the winner had submitted an evaluation form. More detailed information about this pilot can be found in [ALP+12] and [DGL+12].

4.2 School Community Interaction Platform

According to the 2013 statistics [Find13], 86 to 97 percent of children between the ages of 12 to 15 years in Sweden are accessing the Internet on a daily basis. At the same time, the use of the Internet has become much more common in Swedish schools in recent years. More specifically, the daily Internet use in schoolwork has increased from 11% in 2009 to 53% in 2013 among the students in the above age group. There has been a similar trend in the use of Social Networks. For example, the statistics show that some children start using social networking sites at the age of eight even though there is a higher minimum age requirement (i.e. 13 years for Facebook). Focusing on the age group of 12 to 15 years, a daily visit at Facebook is done by 59% of the boys and 68% of the girls in 2013. The observed growth in use of the Internet and social networks among the Swedish teenagers affirms the choice of the pilot environment by ABC4Trust.

The Norrtullskolan school of Söderhamn in Sweden hosts the school trial of ABC4Trust, where a privacy friendly platform, built upon Privacy-ABCs, is deployed to boost the communication between the pupils, their parents and the school personnel. The platform is developed as a web-based application to be used for chat communication, counselling, political discussions and exchange of sensitive and personal data between pupils, parents, and school personnel such as teachers, administrators, coaches, nurses etc.

The community platform uses an abstract model called "Restricted Area" (RA) that provides the virtual environment for the aforementioned activities. Every user can initiate such a private space and define access policies in order to restrict the participation to her desired target group. For example, a teacher can create an RA with "Chat" functionality to collect the opinions of the pupils about his teaching methods and limit the access to this chat room to participants of a specific class. In this case the pupils of that class can join the discussion and stay anonymous under an "Alias" while the other students from the school are prohibited to enter this chat room.

In general, the participants can choose to interact with the system using an alias or their real identity. In this regard, the platform also supports the cases where identification of users is desired. For example, each participant owns a private RA that is used similar to an inbox for receiving messages or documents that are specifically addressed to this person. In order to access this RA, a user must disclose her identity and prove her ownership of the RA. The third type of authentication offered in this platform is conditional anonymity. An RA can be defined to be "Inspectable", meaning that the authentication token gives the possibility to the "School Inspection Board" to reveal the identity of a user under specific (extreme) circumstances that have been announced in advance. In that case, the participants are notified about the nature of this RA before entering it and can decide whether they want to join the activity of not. This mechanism is established to assist the school to fulfil some of its legal obligations such as controlling bullying threats.

All the pilot participants are equipped with smartcards and smartcard readers so that they can use the platform from their personal computers as well as the computers in the schools. The smartcards are preloaded with a set of credentials that specify their basic information such as first name, last name, and birthdate, their roles (i.e. pupil, parent, teacher, nurse, etc.), the classes and courses that the pupils are enrolled in. Consequently, the access policies for the RAs should be defined based on the attributes in the credentials.

Due to the wider range of activities in this trial compared to the university trial, the first round of this pilot started in May 2013 in a smaller scale to better investigate the scalability of the platform and thus be able to address its shortcomings before a larger scale deployment. In this round 24 students used the system to accomplish the given tasks. Their feedback was collected and later reflected in the next deployment. The second round of the pilot was launched in October 2013 with 378 participants consisting of 52 school personnel, 121 pupils, and 205 parents. The trial will continue until the end of January 2014. More detailed information about this pilot can be found in [BGOZ12] and [ABD+13].

5 The Reference Implementation

The main purpose of the reference implementation is to provide a common platform, which exposes a unified architecture for selected Privacy-ABC systems and enable the deployment of the reference implementation in pilots involving actual end-users. Furthermore the refer-

ence implementation is a research vehicle for understanding the interoperability issues of the selected ABC systems.

The reference implementation faithfully implements and realises most of the architecture, protocol, and API for Privacy-ABCs as defined in [CKL+11]. It is not a goal of the reference implementation per se to be tuned towards to high performance. Also the reference implementation implements the entire architecture, and as such is very versatile. The reference implementation can easily be deployed, but it will require some tailoring to fit the specific needs of a particular application. The main modification points will be user interface, smartcard application, storage (of keys, credentials, parameters etc.), and perhaps performance. An example is the user interface, which can be simplified in simple application cases.

Figure 4 depicts the communication between parties in an example deployment of the reference implementation. It shows that the user communicates with any other party (i.e. Issuer, Verifier, Inspector, and Revocation Authority) in the system in the same way.

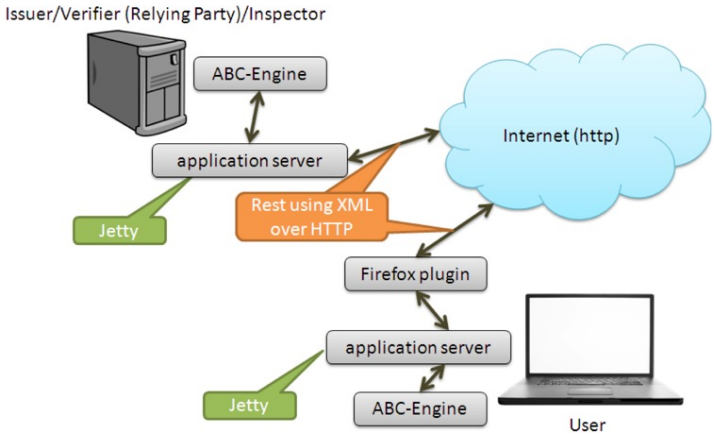

Figure 4: Deployment of the ABC4Trust reference implementation

The core end-point at any involved party will always be the ABCE. The ABCE is written in Java since Java gives easy interoperability between platforms. Furthermore, integration with some of the crypto libraries (i.e. Idemix) written in Java is facilitated.

To get a working Privacy-ABC system running, a number of parameters/resources have to be distributed amongst the parties. This includes public key material, credential specifications etc. In order to simplify this process, certain helper classes have been developed. Given various resources, these helpers will populate the key managers and other components used by an ABCE and finally return an initialized ABCE. Each of the helpers is designed for a specific purpose, i.e. User ACBE, Issuer ABCE or Verifier ABCE. The helpers and the produced ABCE can either be used directly or be wrapped into a web-service to allow easy use in user applications.

In order to run the services on each party, an application server is needed, and we chose Jetty for this purpose. This was a natural choice because Jetty is also written in Java. The communication between the entities is done via XML since XML has widespread support and can easily be checked for integrity.

The reference implementation contains a browser plugin (for Firefox and IE) that enables the reference implementation services to talk to the applications. Without the browser plugin, the services would have to resort to cross-site scripting which would not work in any modern

browser. Thus, we encapsulate the possible calls to the user's local web service within the browser plugin. This also ensures that we only call the service in the correct way, removing a lot of potential bugs. The browser plugin also offers the functionality to change the users PIN code, unlock the card with the PUK code if the card has been locked due to 3 incorrect PIN inputs. The user can manage her credentials, i.e. view or delete them. Furthermore, the user has the possibility to request a backup or restore the content of the smartcard. In addition to that some debugging information can be obtained via the browser plugin.

A user interface for selecting credentials and pseudonyms is developed as part of the reference implementation. The user interface is presented to the user in case a user needs to present credentials and/or pseudonyms to a verifier.

Along with the reference implementation, ABC4Trust offers a demonstration example that shows how to integrate and deploy the reference implementation in a web setting. The example shows a scenario where a country can issue identity cards to its inhabitants and based on these cards the inhabitants can access a service.

6 Smartcard Integration

6.1 Why smartcards?

In the reference implementation it is possible to use smartcards for storing the user's credentials and her secret key. Having the credentials on a portable device allows the user to use her credentials from any computer that the ABC User service is installed, which was an important feature in the projects' pilots. For example in the school pilot, it allowed the pupils to login to the community interaction platform from home or at school.

Having the user's secret key on the smartcard greatly increases the security of the system. Not only because smartcards are tamper-resistant, making it very hard to retrieve a user's secret key from a smartcard, but also because a malicious adversary needs to get hold of both the smartcard *and* the users PIN-code in order to be able to impersonate her. In addition to that, storing the secret keys on smartcards prevents the users from sharing credentials.

For a more detailed discussion about the benefits of using smartcards, see [Bran00].

6.2 Smartcard related Challenges

Despite of their convenient usage, smartcards can be very surprising during the development phase. In this section we briefly talk about the challenges that we faced during the ABC4Trust projects with regard to the smartcards.

The very first plan of the ABC4Trust project was to use an upcoming novel smartcard platform, which was offering very desirable computation and storage capabilities as well as access to the low level APIs. Unfortunately, after the first release, it turned out, that due to a hardware bug in the communication interface, the platform would not be ready in time to be used in the project. Therefore, the project decided to investigate other available options.

In the first university trial, we used a smartcard from ZeitControl, which turned out to have a multitude of problems. The biggest problem was a random error that we never found the cause for. However, the card was previously detected to have issues with RAM-handling,

which may have been the problem. Later we found out that the card also does not support all the claimed functions.

An implementation challenge at that point was the synchronization between the two CryptoEngines when using the smartcard. We used Java for the Idemix implementation and .NET for the U-Prove part of the ABCE, and therefore two different drivers were needed to communicate with the smartcard. Although this never occurred at the same time, it still caused problems with releasing the lock from the smartcard. Switching to a pure Java implementation after introduction of the new crypto architecture resolved the issue.

Different ways of handling hash functions by U-Prove and Idemix were another challenge that we had to deal with in the early phase. The two engines disagreed on the way to hash a value, so we needed to implement two different hash functions on the smartcards.

As the design of the pilots progressed, we encountered difficulties with the storage space available. There simply was not enough space to support the scenarios in the school trial. Due to this issue and also our interest to increase the performance, the project decided to change the platform to the MULTOS smartcards.

Switching to the MULTOS cards was not a very straightforward process since the developers discovered a variety of issues. More specifically, some functions that MULTOS claimed in the specifications were not implemented on the hardware. In addition to that, some functions did not work in the way they were supposed to, e.g. the modular multiplication. Nevertheless, the developers managed to workaround the issues and ended up with a fully working smartcard application.

Apart from the technical difficulties mentioned above, there have been some challenges in the scenario design process for the pilots with regards to smartcards. The project decided to enable a backup and restore feature in case of stolen, broken or lost smartcards, which posed several issues. In the first place, appropriate measures had to be taken to prevent manipulation of the backup images and preserve their secrecy. In case of the project pilots, there was no need to include the credentials in the backup since they could be always re-issued.

In the university pilot, we relied on a “counter” mechanism for recording the attendance records on the card. If the backup only contains the attendance information, it could be misused to distribute the backup to other students who could then restore the image and suddenly have a working card for evaluation, even though they really did not participate enough in the lectures. As a result we embedded the “deviceID” in the backup image and programmed the smartcard in a way that it rejects the backup images from smartcards belonging to other students (a new card is initialized with the same deviceID as the previous one). This removes the cloning possibility, but an adversary can still misuse the system in another way: The adversary could show up as a new student and evaluate the course again, if she claims her card stolen and gets a new card after submitting her first evaluation. We addressed this threat by limiting the time when one can request a new card to the period before the evaluations starts. The scenario is immune in this case since the credentials will be revoked once the smartcard is reported lost.

In case of the school pilot the backup scenario was slightly more complicated. The pilot needs to ensure that pupils do not lose their aliases in case of a broken card since they are stored only on the smartcard and they are bound to the secret key of the user. As a result, the backup image must contain both the secret key and the alias list in order to transfer them to the new card. The problem was to prevent someone from cloning a card. An adversary can claim her

card stolen, and get a new one with the same deviceID enabling her to restore the backup image. She can use the new card to obtain new credentials (as the old ones are revoked) and then clone everything to the previous card (with the same deviceID). Essentially this problem cannot be easily fixed apart from not doing backup at all. However, in a pilot environment with 12-15 years old pupils, it makes sense to take the risk of cloned cards rather than going for expensive and complicated solutions.

6.3 Performance

As a better response time is always desired in the pilots, we investigated on the performance of the applications. It turned out that a main performance bottleneck was the smartcard, where especially downloading data from the smartcard was cumbersome, being responsible for 46% of the total time. The graph in Figure 5 shows that for a presentation downloading data from the smart card and smartcard operations were responsible for more than 80% of the total time.

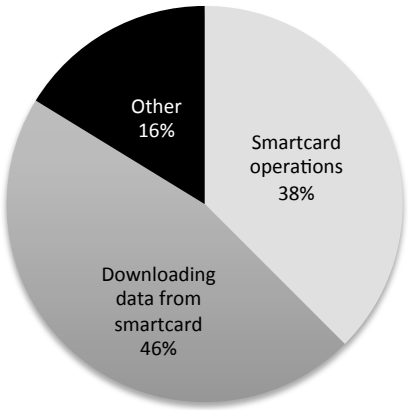

Figure 5: Distribution of time consumption during a presentation

The presentation analysed involved two credentials. The key size was 2048 bits and the total time spent on the presentation was 24.4 seconds. The test was conducted on an Intel duo core 2.2 GHz with 2 GB RAM, running Windows 7 32-bit.

The amount of data that needs to be downloaded from the card decreases on a second presentation on the same PC due to some of the data being cached. It is worth noting that some of the data being downloaded are not secret data, and in principle could be retrieved from another faster source.

As mentioned earlier, smartcards were chosen because they offer a portable and tamper-resistant way of storing keys and credentials. If another device offered the same security *and* better performance, for example a smart phone with a hardware backed key store, it could be used instead, giving a better total performance of the application, not to mention the improved usability of not having to carry an extra token. It is the intentions of the project to perform an analysis and develop a prototype of these possibilities.

7 Conclusion and Outlook

The ABC4Trust project has successfully tested the feasibility of implementing Privacy-ABCs on smartcard for real life and large-scale deployments. In this regard, the informal feedback

about the trials is positive and quite a few of the partners are eager to plan larger trials. Therefore, one can expect wider adoption of Privacy-ABCs in real environment.

From our experience, when it comes to development of high performance and rich functionality applications on smartcards, one could still experience the problem of immaturity of smartcard platforms. As a lesson learnt, the paradigm of universal open access high performance smartcards has not realised yet. Even tough smartcards troubled us during the development phase there is no proper replacement that gives the same level of secure computation and ease of use for the users. As mentioned earlier, ABC4Trust is investigating the possibility of using smartphones as the user token as well, but of course the known issues of smartphones make clear, that this may be no easy exercise.

Literature

[ABD+13] Abendroth, J., Bcheri, S., Damgaard, K., Ghani, H., Luna, J., Læssøe Mikkelsen, G., Moneta, M., Orski, M., Suri, N., Zwingelberg, H.: *D6.2 Necessary hardware and software package for the school pilot deployment*, Download: https://abc4trust.eu/download/ABC4Trust-D6.2.Hard-and-Software-Package-for-School-Pilot.pdf, 2013.

[ALP+12] Abendroth, J., Liagkou, V., Pyrgelis, A., Raptopoulos, C., Sabouri, A., Schlehahn, E., Stamatiou, Y., Zwingelberg, H.: *D7.1 Application Description for Students*, Download: https://abc4trust.eu/download/ABC4Trust-D7.1-Application-Description-Students.pdf, 2012.

[BGOZ12] Bcheri, S., Goetze, N., Orski, M., Zwingelberg, H.: *D6.1 Application Description for the school deployment,* Download: https://abc4trust.eu/download/ABC4Trust-D6.1-Application-Description-School.pdf, 2012.

[Bran00] Brands, S.: *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, 2000, Pp. 15-19.

[Bran93] Brands, S.: *Untraceable off-line cash in wallets with observers (extended abstract)*. In: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, Springer, 1993, Pp. 302–318.

[CaLy01] Camenisch, J., Lysyanskaya, A.: *An efficient system for non-transferable anonymous credentials with optional anonymity revocation*. In: Birgit Pfitzmann: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology Springer, 2001, Pp. 93-118.

[CaLy04] Camenisch, J. and Lysyanskaya, A.: *Signature schemes and anonymous credentials from bilinear maps.* In: Matt Franklin: Proceedings of the 24th Annual International Cryptology Conference, Springer, 2004, Pp. 56–72.

[Chau85] Chaum, D.: *Security without identification: Transaction systems to make big brother obsolete*. In: Peter J. Denning: Communications of the ACM, ACM, 1985, Pp. 1030-1044.

[CKL+11] Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., Zwingelberg, H.: *D2.1 Architecture for Attribute-based Credential Technol-*

ogies. Download: https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.2.pdf, 2011.

[DGL+12] Damgaard, K., Ghani, H., Goetze, N., Lehmann, A., Liagkou, V., Luna, J., Læssøe Mikkelsen, G., Pyrgelis, A., Stamatiou, A.: *D7.2 Necessary hardware and software package for the student pilot deployment*, Download: https://abc4trust.eu/download/ABC4Trust-D7.2.Hard-and-Software-Package-for-Student-Pilot.pdf, 2012.

[Find13] Findahl, Olle: *Swedes and the Internet*. Download: https://www.iis.se/docs/Swedes_and_the_internet-2013.pdf, 2013.

[Rann00] Rannenberg, Kai: *Multilateral Security – A concept and examples for balanced security*; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3

[SaKR12] Sabouri, A., Krontiris, I., Rannenberg, K.: *Attribute-Based Credentials for Trust (ABC4Trust)*. In: Simone Fischer-Hübner et. al.: Proceedings of 9th International Conference on Trust, Privacy and Security in Digital Business, Springer, 2012, Pp. 218-219.

CV

Ahmad Sabouri received the B.Sc. degree in Computer Engineering in 2009 from the University of Tehran and the M.Sc. in Information Networking in 2011 from Carnegie Mellon University. Since then, he is a scientific researcher and doctoral candidate with the Deutsche Telekom Chair of Mobile Business and Multilateral Security at Goethe University Frankfurt.

Kontakt

Ahmad Sabouri
Grüneburgplatz 1
60323 Frankfurt am Main
Tel. +49 69 798 34705
Fax +49 69 798 35004
E-Mail: ahmad.sabouri@m-chair.de

CV

Jonas Lindstrøm Jensen received the M.Sc. degree in mathematics in 2009 and the Ph.D. Degree in number theory in 2012, both at Aarhus University, and has since 2013 worked at the Alexandra Institute as R&D specialist.

Kontakt

Dr. Jonas Lindstrøm Jensen
The Alexandra Institute
Aabogade 34

8200 Aarhus N, Denmark
Tel. +45 51 72 89 30
E-Mail: jonas.l.jensen@alexandra.dk

CV

Kasper Lyneborg Damgård received his M.Sc. in computer science in 2011from the University of Aarhus. Since then, he has been employed by the Alexandra Institute A/S as a research and innovation specialist in the security lab focusing on MPC and it-security.

Kontakt

Kasper Lyneborg Damgård
The Alexandra Institute
Aabogade 34
8200 Aarhus N, Denmark
Tel. +45 30 55 33 86
E-Mail: kasper.damgaard@alexandra.dk

CV

Janus Dam Nielsen received the M.Sc. degree in computer science and the Ph.D. degree in programming languages from Aarhus University, Aarhus, Denmark, in 2006 and 2009, respectively. Since then, he has been with the Alexandra Institute A/S, Aarhus, Denmark, where he is currently Senior Research and Innovation specialist. His main areas of research interest are it-security, identity management, and secure computation.

Kontakt

Dr. Janus Dam Nielsen
Kasper Lyneborg Damgård
The Alexandra Institute
Aabogade 34
8200 Aarhus N, Denmark
Tel. +45 40 83 09 10
E-Mail: janus.nielsen@alexandra.dk

CV

Kai Rannenberg holds the Deutsche Telekom Chair of Mobile Business & Multilateral Security since 2002. Before he was with the System Security Group at Microsoft Research Cambridge, UK, focussing on “Personal Security Devices & Privacy Technologies”. Since 1991 Kai is active in the ISO standardization of IT Security and Criteria. Since March 2007 he is Convenor of the ISO/IEC JTC 1/SC 27/WG 5 Identity management and privacy technologies". Kai is active in the Council of European Professional Informatics Societies (CEPIS) chairing its Legal & Security Issues Special Interest Network (CEPIS LSI) since 2003. Kai's research interests include: Mobile applications and Multilateral Security in e.g. Mobile Business, Mobile Commerce, Mobile Banking, and Location Based Services.

Kontakt

Prof. Dr. Kai Rannenberg
Grüneburgplatz 1
60323 Frankfurt am Main
Tel. +49 69 798 34701
Fax +49 69 798 35004
E-Mail: kai.rannenberg@m-chair.de