ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-Life

Ahmad Sabouri, Kai Rannenberg

▶ **To cite this version:**

Ahmad Sabouri, Kai Rannenberg. ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-Life. Jan Camenisch; Simone Fischer-Hübner; Marit Hansen. Privacy and Identity Management for the Future Internet in the Age of Globalisation: 9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Patras, Greece, September 7–12, 2014, AICT-457, Springer, pp.3-16, 2015, IFIP Advances in Information and Communication Technology (TUTORIAL), 978-3-319-18620-7. ⟨10.1007/978-3-319-18621-4_1⟩. ⟨hal-01431588⟩

HAL Id: hal-01431588

https://inria.hal.science/hal-01431588v1

Submitted on 11 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons CC BY 4.0 - Attribution - International License

ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-life

Ahmad Sabouri and Kai Rannenberg

Deutsche Telekom Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt,
Theodor-W.-Adorno-Platz 4, 60323 Frankfurt, Germany
{Ahmad.Sabouri,Kai.Rannenberg}@m-chair.de
https://www.abc4trust.eu

Abstract. Security of the Identity Management system or privacy of the users? Why not both? Privacy-preserving Attribute-based Credentials (Privacy-ABCs) can cope with this dilemma and offer a basis for privacy-respecting Identity Management systems.
This paper explains the distinct features of Privacy-ABCs as implemented in the EU-sponsored ABC4Trust project via example usage scenarios from the ABC4Trust pilot trials. In particular, it aims for a deeper insight from the application perspective on how Privacy-ABCs can support addressing real-life Identity Management requirements while users' privacy is protected.

1 Introduction

As using online services penetrates deeper in our everyday life, lots of trust-sensitive transactions such as banking and shopping are carried out online and many users would prefer to perform their transactions online rather than follow the traditional procedures. In this regard, the biggest challenges are to deal with proper user authentication and access control, without threatening users' privacy.

The currently employed Identity Management systems have limitations when it comes to users' privacy. Nevertheless, new promising techniques, known as Privacy-ABCs, have emerged to enable privacy-respecting Identity Management solutions. In this regard, the ABC4Trust EU Project[1] put considerable effort to foster adoption of such technologies by designing an architectural framework for Privacy-ABCs, implementing it, and trialling it in two pilots.

In this paper, we aim to elaborate on the most important features provided by Privacy-ABCs via real-life example usage scenarios from the ABC4Trust trials. The rest of this paper is organized as follows. Section 2 describes the issues of the existing Identity Management systems. In Section 3, we introduce Privacy-ABCs and explain how they work. Later we describe the ABC4Trust pilots in

[1] https://abc4trust.eu

Section 4. Section 5 focuses on the most important features of Privacy-ABCs and there we elaborate how these features help to deal with the requirements of the pilots. Later in Section 6, we briefly describe the ABC4Trust architecture for Privacy-ABCs and then conclude the paper in Section 7.

2 Privacy Issues in Identity Management

This chapter describes the privacy issues in nowadays digital identity management systems. Although most of the commonly used strong authentication techniques offer a suitable level of security, they are not appropriately designed to protect the privacy of the users. For instance, use of X.509 [1] certificates causes "Over-identification" by mandating the users to reveal all the attested attributes in the certificate to preserve the validity of the digital signature even if only a subset of attributes is required for the authentication purpose. Apart from this, the online users also have to be able to compartmentalize their activities in different domains and prevent profiling by both Service Providers and Identity Service Providers (IdSP). Evidently, the static representation of X.509 certificates fails to address the problem and makes it possible to trace users' online activities.

Using online authentication and authorization techniques such as OpenID [2], SAML [3], Facebook Connect [4], and OAuth [5] could support the minimal disclosure principle, as they enable the user to provide the Service Provider with only the requested information rather than the whole user's profile stored at the IdSP. However, all these protocols suffer from a so-called "Calling Home" problem, meaning that for every authentication transaction the user is required to contact the IdSP (e.g., Facebook, OpenID Provider). This introduces privacy risks to both users and Service Providers. More specifically, it would not be difficult for the IdSP to trace the user and profile her online activities due to the knowledge it gains about the Service Providers she visits. Moreover, the IdSP can collect a considerable amount of information about a Service Provider by analysing the profile of the users who request to authenticate to that specific service.

In summary, when designing identity management and access control systems inspired by the paradigm of Privacy by Design, the following concepts related to data thriftiness shall be of direct or indirect interest for bodies working on privacy-friendly ecosystems:

- Partial Identities and Partial Identifiers: More and more public and private parties are trying to overcome the natural borders between domains of activities, making users ever more transparent from ever more perspectives, e.g for many Service Providers offering services that relate to different parts of users' lives. Partial Identities and Partial Identifiers become more and more important for users to retain these borders by reducing the dangers of unwanted linkability across domains. Therefore the definition of Identity as a "set of attributes related to an entity", that has been globally standardized in the Part 1 of the framework for identity management [6] developed

by ISO/IEC JTC 1/SC 27/WG 5 "Identity Management and Privacy Technologies", is useful for designing privacy-respecting identity management.
- Unlinkability: Unlinkability is related to Partial Identities and Identifiers, but in this context focusses on multiple uses of services within one domain. It ensures that a user may make multiple uses of resources or services without others being able to profile these activities.
- Minimal Disclosure: It is a common practice that Service Providers rely on the information about users provided by other entities that have an authentic profile of users' attributes. However, these entities typically possess a richer collection of information than is needed by the respective Service Provider. In this regard, the users should have the possibility to calibrate the amount of disclosed information to the requested set only. Therefore on the side of the Service Providers risk management processes compatible with the minimal disclosure need to be established.

3 Privacy-preserving Attribute-based Credentials (Privacy-ABCs)

Privacy-ABCs can offer strong authentication and a high level of security to Service Providers with user privacy preserved, so that it follows the paradigm of Multilateral Security [7]. 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. Prominent instantiations of such Privacy-ABC technologies are Microsoft U-Prove[2] [8] and IBM Idemix[3] [9].

A Credential is defined to be "a certified container of attributes issued by an Issuer to a User" [10]. An Issuer vouches for the correctness of the attribute values for a User when issuing a credential for her. For example, a school can issue an "Enrolment Credential" for a pupil, which contains several attested attributes such as first name, last name, student id and the enrolment year.

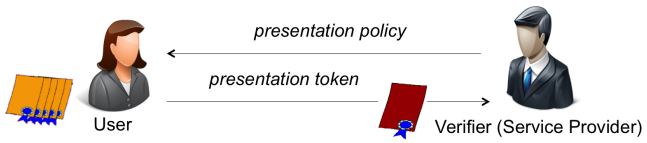

Fig. 1. A sample presentation scenario

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

[2] `http://www.microsoft.com/uprove`
[3] `http://www.zurich.ibm.com/idemix/`

Service Provider performs a so-called Verifier role and expresses its requirement for granting access to the service in the form of a Presentation Policy. In the next step, the User needs to come up with a combination of her credentials to derive an acceptable authentication token that satisfies the given policy. After the Verifier confirms the authenticity and credibility of the Presentation Token, the User gains access to the corresponding service. It is worth noting that the human User is represented by her UserAgent, 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. In addition, the User may also bind credentials to special hardware tokens, e.g. smart cards, to improve security.

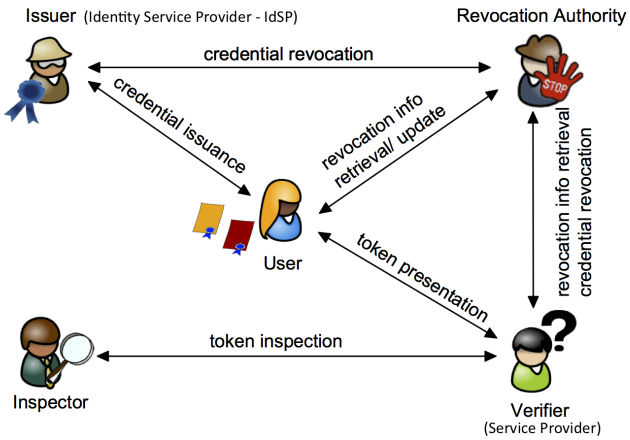

Fig. 2. Entities and relations in the Privacy-ABC's architecture [10]

As Figure 2 shows, in addition to *User*, *Issuer*, and *Verifier*, two other (optional) entities are involved during the life-cycle of Privacy-ABCs [10]. The Revocation Authority is responsible for revoking issued credentials. Both the User and the Verifier must obtain the most recent revocation information from the Revocation Authority to generate presentation tokens and respectively, verify them. The Inspector is an entity who can de-anonymize presentation tokens under specific circumstances. To make use of this feature, the Verifier must specify in the presentation policy the conditions, i.e., which Inspector should be able to recover which attribute(s) and under which circumstances. The User is informed about the de-anonymization options at the time that the presentation token is generated and she has to be involved actively to make this possible.

The EC funded project Attribute-based Credentials for Trust (ABC4Trust)[4] brought all the common features of the existing Privacy-ABC technologies together and provided a framework abstracting from the concrete cryptographic realization of the modules underneath. This gives software developers the flexibility to build Privacy-ABC enabled systems without concern about what cryptographic schemes will be employed at the bottom layer. As a direct result, the Service Providers are free to choose from those concrete cryptographic libraries that implement the ABC4Trust required interfaces, and plug them into their software solutions. This helps to avoid a lock-in with a specific technology, as the threat of a lock-in reduces the trust into an infrastructure.

4 Trialling Privacy-ABCs in Real Life Applications

The ABC4Trust project realized the first ever implementation of Privacy-ABC systems in production environments and gathered experiences on operation, interoperability, user acceptance, and so forth in two specific trials. Having these two pilots gave the opportunity to test Privacy-ABCs use and performance with two user groups of differing skills and needs. One user group were were students at a Greek university, whereas the other group were pupils at a school in Sweden. The trials were designed quite different in order to cover a broad variety of requirements and thus as well credentials.

4.1 Online Course Evaluation

A standard practice 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. However, both the students and the professors have legitimate concerns about the process of course evaluation. The students may be worried about their identities being linked to their evaluation forms, resulting in negative impacts on their grades or education records. Meanwhile, professors consider a minimum level of participation in the lectures to be necessary for the students to get the real experience of the course and therefore to be eligible to evaluate it. The scenario becomes even more complex in terms of security, privacy, and trust, when electronic evaluation is desired.

Privacy-ABCs could help to address the aforementioned requirements in an online course evaluation system. In this regard, ABC4Trust executed two rounds of trials in Fall 2012 and Fall 2013 at the Patras University in Greece to realize such a system. Whilst the identity and privacy of the students were protected, the opinions of the students, who had attended more than a certain number of lectures, were collected via an evaluation portal.

At the beginning of the semester, the pilot participants were provided with their start-up kit including smart cards and necessary login information enabling the participants to bootstrap their access to the pilot system, register their smart cards and obtain their Privacy-ABCs from the identity management system.

[4] `https://abc4trust.eu`

After the initialization actions were taken at the beginning of the semester, the students could record their participation in the lectures on their smart cards. 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 led to privacy breaches. Therefore, the attendance records were only stored on the smart cards of the students and not anywhere else.

During the evaluation period, the student could access the evaluation form online 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 smart card could produce a Privacy-ABCs presentation proof that attested the student's eligibility to evaluate the course. While it was not possible to link the evaluations to the identity of the participants, the authentication step was designed in a way that the evaluation portal could prevent the same users from submitting multiple evaluations.

The second round of the trial aimed to further test the Privacy-ABCs' features developed in ABC4Trust in an actual deployment environment. New features such as revocation of credentials, advance issuance, and inspection of tokens (de-anonymization) were implemented and introduced into the pilot. The scenarios of the first round were extended in order to best integrate these new features. More specifically, after the students submitted their evaluations, they could receive a new credential allowing them to later take part in a privacy-friendly tombola. When the winner was selected, her identity was revealed through the inspection of her presentation token. In this phase, there was no privacy risk for the winner with regard to the evaluation she provided, as the only information one could learn was that the winner had submitted an evaluation form.

4.2 School Community Interaction Platform

The Norrtullskolan school in Söderhamn, Sweden, hosted the second pilot of ABC4Trust, where a privacy-friendly communication platform, built upon Privacy-ABCs, was deployed to encourage communication between pupils, their parents and school personnel. The pupils were able to authenticate themselves in order to access restricted online activities and restricted information. Moreover, they were able to remain anonymous when they asked private and sensitive questions to school personnel, while simultaneously assuring the school personnel that they were communicating with the authorised pupils of the respective school or class.

The platform was 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, and nurses. This pilot specially helped to gather information on the usability of the Privacy-ABC systems under especially challenging usability conditions posed by children users. Due to the wide range of activities in this trial, the pilot was operated in two rounds where the first round was on a smaller scale to investigate the scalability of the platform and thus be able to address its shortcomings before a larger scale deployment.

All the pilot participants were equipped with the necessary hardware so that they could use the platform from their personal computers as well as the computers in the school. The smart cards were preloaded with a set of credentials that specified the participants' basic information such as first name, last name, and birth-date, their roles (i.e. pupil, parent, teacher, nurse, etc.), the classes and courses that the pupils were enrolled in, consequently giving the chance to define the access policies based on these attributes in the credentials.

The community interaction platform used an abstract model called "Restricted Area" (RA) that provided the virtual environment for the aforementioned communication activities. Every user could initiate such a private space and define access policies in order to restrict the participation to her desired target group. For example, a teacher could create an RA with "Chat" functionality to collect the opinions of the pupils about her teaching methods and limit the access to this chat room to participants of a specific class. In this case, the pupils of that class could join the discussion without being identified, while the other students from the school were prohibited to enter this chat room.

5 Privacy-ABCs Features

In this section we introduce some of the most important features of Privacy-ABCs along with examples of their usage in the real scenarios of our trials. In summary, we talk about pseudonyms and their relation to partial identities, minimal disclosure, untraceability and unlinkability, advance credential issuance techniques, Inspection process, and security mechanisms.

5.1 Multiple Pseudonyms

Using X.509 certificates, a user is identified by her public key, which is associated with her secret key. The issue here is that for every secret key there is only one public key. As a result, the user will be linkable across different domains where the public key is used, unless she accepts the hassle of managing multiple key pairs. The concept of "pseudonyms" in Privacy-ABC system can be considered as equivalent to public keys. However, the major difference is that "many" different unlinkable pseudonyms can be derived from a single secret key, allowing the user to establish partial identities in different domains that are not possible to correlate.

The Söderhamn pilot of ABC4Trust heavily benefited from pseudonyms to realize the concept of "Alias" in their School Community Interaction Platform.

Every pupil has the possibility to appear in the online community under various human friendly nicknames (aliases) representing partial identities. These aliases are bound to Privacy-ABC pseudonyms behind the scenes. Once a user requests a new alias, the system checks the database to ensure that the alias is not already registered. When there is no conflict, the user submits a pseudonym bound to the selected alias name to be registered in the database. Afterwards, whenever the user desires to login under that alias, the system requires to produce and prove ownership of the same related pseudonym. As a result, no impersonation is possible and nobody can figure out whether two aliases belong to the same person.

5.2 Identifying Returning Users

Even though unlinkable Privacy-ABC pseudonyms are very attractive to support users' privacy, sometimes a system may fail delivering its service if a certain level of linkability is not provided. To elaborate more on such cases, we take the example of the ABC4Trust Patras pilot, where an online course evaluation system was implemented.

A privacy-respecting course evaluation system must allow the students to fill the questionnaire and express their opinion without being identified. However, the result could be manipulated if the students have the possibility to establish multiple partial identities to submit multiple evaluations under different pseudonyms, and therefore positively or negatively influence the aggregated results. Thus, for a correct and accurate delivery of the service, the course evaluation system must be able to link the users to their previous visits of the system and only allow them to "update" their evaluations, instead of submitting a new entry. At the same time, there should not be a way to learn about the identity of the students.

"Scope-exclusive" pseudonyms are special types of Privacy-ABC pseudonyms that enable the Service Provider to force the users to show the same pseudonym given the same "scope" string. Therefore, whenever the users visit the course evaluation portal, they face a policy requiring a scope exclusive pseudonym for a fixed scope. As a result, they are obliged to produce the same pseudonym value every time, allowing the system to recognize a returning user.

5.3 Minimal, Untraceable, and Unlinkable Presentation of Credentials

In a Privacy-ABC system, users can receive certified claims about their attributes in the form of credentials. For example, a Civil Registration Authority is entitled to issue authentic credentials attesting name, last name, birth-date, etc., representing an ID card.

Privacy-ABCs provide three distinct features to their users. Let's take the School Credential of the Söderhamn pilot as the basis for our examples here. The School Credential (also called CredSchool) is equivalent to a membership card and contains the first name, last name, birth-date, and the school name. As

mentioned earlier, the pupils could login to the system using a human friendly nickname, called alias, which is not linkable to their real identities. In order to participate in a school-bound activity, such as a political discussion, a sample access policy would require a proof that they are from the same school (i.e. Norrtullskolan).

X.509 certificates require users to present their certificate as it is needed to preserve the integrity of the signature. This urges the users to disclose their first name, last name, and the birth-date even though only the school name was needed. Conversely, Privacy-ABCs support minimal disclosure allowing the users to selectively disclose a subset of the attributes from their credentials. In the example of the Söderhamn pilot, the pupils could use their CredSchool to reveal only the school name whilst keeping the other attributes hidden. In this way the system did not learn any further information than needed. Moreover, Privacy-ABCs support "predicates over attributes" enabling the users to prove some facts about their attributes without actually revealing them. For instance, the pupils could prove that their birth-date from the CredSchool is before a given date and therefore they are older than a certain age, and still keep their actual birth-date hidden.

Another advantage of Privacy-ABCs can be better explained when focusing on the static representation of X.509 certificates. An X.509 user could be immediately identified when the Service Provider and the certificate issuer collude. In another word, the use of the credentials is traceable by the issuer due to the static representation of the certificates during the issuance and the presentation steps. Despite, Privacy-ABCs experience some transformations between the issuance and presentation phase so there is no way to trace their usage, unless the revealed attributes give such an opportunity. In our example, the pupils could use their CredSchool to prove that they are part of the Norrtullskolan, and this piece of information would not allow a colluding credential issuer to identify the users.

Similarly, the same static nature of X.509 certificates enables another privacy threat to the users. It would allow the Service Providers to link different transactions of the same users and build a profile. This would not be possible with Privacy-ABCs as the users are able to produce unlinkable tokens from their credentials for each transaction. In our example scenarios, a pupil could use the same CredSchool to make presentations about their school name when appearing under different aliases in the system and ensure that this would not introduce any linkability between their aliases.

5.4 Blind Transfer of Attributes

Let's introduce an example scenario from the ABC4Trust Patras pilot to better elaborate on the feature of blind transfer of attributes. To encourage the pilot participants to continue to the last step, we announced a tombola to take place at the end of the trial for those who submitted their evaluation of the course. The approach was to issue to the students a Tombola Credential after submission of their evaluation. However, the new credential had to contain the matriculation

number of the student. This looks challenging as the students were not identified when interacting with the portal.

Advanced credential issuance techniques of Privacy-ABCs support a feature called "carried-over attribute" that allows an issuer to issue a credential containing an attribute value transferred from another credential that the user holds, without learning the attribute value. Therefore, in the Patras trial, after submitting the evaluation form, the Tombola Credential Issuer could issue credentials to the users and transfer the matriculation number from their University Credential into it without getting to know what the matriculation number is.

5.5 Recovering the Identity via Inspection

On the first look, the Inspection feature of Privacy-ABCs may be misinterpreted as a back door to the provided anonymity. Thus explaining and using this concept and its processes requires extra care. The first important point to mention about the Inspection is that it would not be possible always, meaning that before anybody would be able to recover the identity of the user behind a transaction, the user should have gone into some agreements and delivered extra information that would make the Inspection technically possible.

When requesting access to a resource protected by Inspection, the users would get informed about the terms and conditions (called Inspection Grounds). If the user accepts the agreement, some additional information, such as a unique identifier in the domain, must be "verifiably" encrypted under the public key of a trusted third party, called Inspector, and has to be embedded in the presentation token delivered to the Service Provider. In case of a misuse, the Service Provider has the possibility to forward this token to the Inspector along with an evidence for the violation of the agreements. The Inspector is responsible for investigating the case and checking whether the claim of violation by the Service Provider holds. Upon confirmation, the Inspector could decrypt the token and recover the identifier.

Inspection is mainly used to achieve accountability. For instance, in the Söderhamn pilot, the school is legally responsible for every infrastructure it provides to the pupils and it must be able to deal with any case that introduces threats to the pupils, such as mobbing. Therefore, a process was designed to allow the pupils report inappropriate contents in the discussion forum. If a forum is protected by Inspection, the "Inspection Board", comprising of the school principal, some teachers and representatives of the pupils, receives the case to judge. If the content is against the terms of use, they send the corresponding token to the Inspector to recover the unique identifier of the pupil.

Inspection can be helpful in other types of scenarios as well. For example, in an online payment process, the credit card number of the customer can be delivered in an inspectable token encrypted under the public key of the bank. In this way, the online shop can ensure that the customer is providing a valid credit card number without actually seeing it. The shop can forward this to the bank to

perform the corresponding transfer of credit. A similar scenario is implemented in the ABC4Trust "Hotel Booking" demo[5].

Another example for a different usage of Inspection was demonstrated in the Patras pilot. As we mentioned earlier, the students would receive a Tombola Credential containing their matriculation number after submitting their evaluation forms. Using this credential they could participate in a tombola. However, this could have caused the threat to identify whoever submitted an evaluation of the course. To make the process privacy-friendly the tombola system required the participants to disclose their matriculation number in an inspectable form and not in clear text. In the end, the Inspector could extract the identity of the winner only and the other students could stay unknown to the system.

5.6 Securing Privacy-ABCs

A typical misuse case is when the users share their credentials in order to let the others benefit from the resources that they normally do not have the necessary credentials to access. Privacy-ABCs try to overcome this problem by offering the "key-binding" feature, which essentially binds a credential to the secret key of the user. Thus, when the users want to lend their credentials, the have to give out their secret key as well. In a Privacy-ABC system, a Service Provider can require a combination of credentials (e.g. a credit card together with a passport) for a presentation and it can enforce that both credentials must be bound to the "same secret key". The "same key as" policy can be applied on pseudonyms as well, meaning that a presentation policy can ask for a credential that is bound to the same secret key as the one used to generate a pseudonym.

Using smart cards as the key/credential storage improves security and portability of Privacy-ABCs. One could rely on the tamper-resistance of smart cards and enhance the security via on-board computation of the operations requiring the secret key. In this way, the secret key never has to leave the card and stays protected as long as the smart card is not tampered with. ABC4Trust also benefited from smart cards in its both pilots and released its smart card firmware on Github[6] to be publicly available.

6 ABC4Trust Layered Architecture

The ABC4Trust architecture has been designed to decompose future 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 algorithms or cryptographic components used underneath. 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.

[5] `https://abc4trust.eu/demo/hotelbooking`
[6] `https://github.com/p2abcengine/`

The interchangeability of Privacy-ABC techniques in the ABC4Trust framework is the outcome of its layered architecture design. Figure 3 depicts part of the high level ABC4Trust architecture where two of the main actors, namely User and Verifier, interact in a typical service request scenario. The core of the architecture is called ABCE (ABC Engine) layer; it provides the necessary APIs to the application layer residing on the top and utilizes the interfaces offered by the bottom layer called CE (Crypto Engine). 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 [10], calls the appropriate ABCE APIs, and exchanges 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.

ABC4Trust also presents a modular model for the crypto layer [10]. The main responsibilities of the Cryptographic Engine are to generate cryptographic key material, issue new credentials by means of a two-party protocol, generate the cryptographic evidence for a Presentation Token to prove that a user satisfies a Presentation Policy, and verify such a proof. This crypto architecture defines the building blocks of Privacy-ABC technologies and their interfaces allowing implementation of additional features and extending the functionalities.

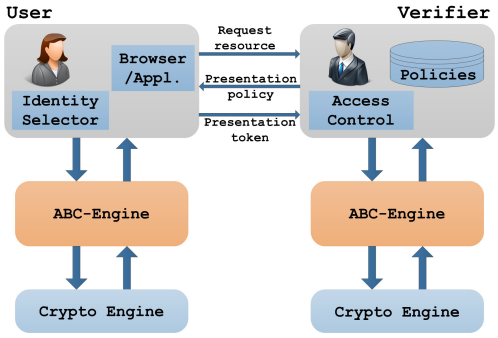

Fig. 3. ABC4Trust layerd architecture, User-Verifier interaction

7 Conclusion and Outlook

This paper has documented the features and the usage of Privacy-ABCs for privacy-respecting identity management considering the interests of the respec-

tive stakeholders. Especially users are enabled to manage their identities and IDs. The examples in Section 5 document privacy-friendly applications in different phases of the businesses process of the two trials, that ABC4Trust conducted.

In some cases identity information flows have been channeled and restricted according to heritage separations of domains, e.g. when enabling users to manage multiple pseudonyms without having to manage multiple key pairs. In some cases new types of channeling and restricting of information flows were enabled by the cryptographic features used in Privacy-ABCs, e.g. the blind transfer of attributes.

In any case it turned out that the definition of Identity as a "set of attributes related to an entity" as globally standardized in the Part 1 of the framework for identity management [6] developed by ISO/IEC JTC 1/SC 27/WG 5 "Identity Management and Privacy Technologies" is useful for designing privacy-respecting identity management.

There are open challenges in the area of assurance tokens which are needed to carry the credentials and process the calculation of presentation tokens. Their design needs to follow several principles

- Enabling the assurance token holder to influence
  - the character and the degree of identification and
  - the amount of identification information;
- Enabling the assurance token to protect itself by e.g. the following features:
  - Ability to verify the controller by e.g. an extra channel to avoid, that an attacker impersonates a controller, e.g. establishes an illegitimate smart card reader to exploit information from the token;
  - A portfolio of communication mechanisms for redundancy to ensure, that any controller, that wishes to access the token, can be verified via an an additional communication channel beyond the channel offered by the controller;
  - Sufficient access control towards relevant data, e.g. a magnet stripe or unprotected chip would not be enough;
  - Enough processing power for complex operations such as cryptographic operations;
- Enabling communication
  - between assurance token holder and assurance token, so that the user can control, what the assurance token is processing and how it is interacting with other entities.

Smart cards are usually able to protect themselves, but their limited user interfaces (even considering a secure reader) makes it challenging for the user to influence the character and degree of identification and the amount of identification information. Moreover the communication between the user as assurance token holder and the assurance token is limited.

Smartphones offer many more options for the interaction between user and assurance token, but they are not as good to protect themselves and the keys stored within them. Reason for this are the complexity of nowadays smartphones

or similar devices and the lack of operating system security. Mobiles phones with more robust protection are urgently needed. Mobile phones with a trusted execution environment (TEE) are a step into the right direction, but the TEE must be securely connected to the user interface making sure, that users' confidential input for the TEE is not misdirected and that output from the TEE is correctly displayed.

References

1. "X.509 : Information technology - open systems interconnection - the directory : Public/key and attribute certificate frameworks," http://www.itu.int/rec/T-REC-X.509/en.
2. "Openid authentication 2.0," http://openid.net/specs/openid-authentication-2_0.html, December 2007.
3. "Assertions and protocols for the oasis security assertion markup language (saml) v2.0," http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, March 2005.
4. "Facebook login," https://developers.facebook.com/products/login/.
5. D. Hardt, "Oauth 2.0 authorization protocol," http://tools.ietf.org/html/rfc6749, October 2012.
6. ISO/IEC 2011, "ISO/IEC 24760-1:2011 Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts, First edition, 2011-12-15," http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.
7. K. Rannenberg, "Multilateral Security - a Concept and Examples for Balanced Security," in *Proceedings of the 9th ACM New Security Paradigms Workshop 2000 (NSPW '00)*. New York, NY, USA: ACM, 2000, pp. 151–162. [Online]. Available: http://doi.acm.org/10.1145/366173.366208
8. S. Brands, *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*. MIT Press, 2000.
9. J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 21–30.
10. P. Bichsel, J. Camenisch, M. Dubovitskaya, R. R. Enderlein, S. Krenn, I. Krontiris, A. Lehmann, G. Neven, J. Dam Nielsen, C. Paquin, F.-S. Preiss, K. Rannenberg, A. Sabouri, and M. Stausholm, "Architecture for Attribute-based Credential Technologies - Final Version," The ABC4Trust EU Project, Deliverable D2.2, 2014, Available at https://abc4trust.eu/download/Deliverable_D2.2.pdf, Last accessed on 2014-11-08.