ABC4Trust Workshop on Core Features of Privacy-ABCs, Practical Use, and Legal Issues

Felix Bieker, Marit Hansen, Gert Læssøe Mikkelsen, Hannah Obersteller

ABC4Trust Workshop on Core Features of Privacy-ABCs, Practical Use, and Legal Issues

Felix Bieker[1], Marit Hansen[1], Gert Læssøe Mikkelsen[2], and Hannah Obersteller[1]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
{fbieker|marit.hansen|hobersteller}@datenschutzzentrum.de
[2] Alexandra Institute AS, Aarhus, Denmark
gert.l.mikkelsen@alexandra.dk

Abstract. The project "ABC4Trust – Attribute-based Credentials for Trust" presented its two pilot trials in a workshop and engaged participants in discussions on the two existing as well as potential future application scenarios. Participants were asked to assess several different scenarios in order to determine when an inspection could be carried out without jeopardizing the potential of Privacy-ABCs to protect users' rights. Their findings have been incorporated in a model inspection process that can be adapted to arbitrary scenarios.

Keywords: ABC4Trust · Identity Management · Attribute-based Credentials · Privacy-ABCs · Conditional Identification · Privacy · Data Protection.

1 Introduction[1]

During the 9th IFIP Summer School on Privacy and Identity Management for the Future Internet in the Age of Globalisation the EC-funded project "ABC4Trust – Attribute-based Credentials for Trust" [1] organized a workshop. Core topics discussed in the workshop were technical, organizational, and legal aspects for using privacy-preserving attribute-based credentials (Privacy-ABCs) in practice.

The workshop took place after two invited talks on Privacy-ABCs and the ABC4Trust project: Professor Kai Rannenberg from Goethe University Frankfurt/Main held a presentation entitled "Identity Management – who is managing what?" (cf. [2]). Dr. Gregory Neven from IBM Zurich introduced "Privacy-preserving authentication: Concepts and policy languages from the ABC4Trust project".

In addition to further familiarizing participants with the instrument of privacy-preserving attribute-based credentials, the workshop served to discuss the existing, as well as potential future application scenarios for Privacy-ABCs and their implementation in a users' rights-centered approach.

[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).

The workshop was organized in three parallel sessions and an additional hands-on session:

- Session I: New Application Scenarios and Storage Devices
  Jonas Lindstrøm Jensen and Michael Bladt Stausholm,
  Alexandra Institute (ALX), Denmark;
  this session was followed by the hands-on session, moderated by the same speakers
- Session II: Optional Features – Inspection and Revocation
  Yannis Stamatiou,
  Computer Technology Institute & Press – "DIOPHANTUS" (CTI), Greece
- Session III: Data Protection and Privacy Requirements for Privacy-ABCs
  Felix Bieker and Hannah Obersteller,
  Unabhängiges Landeszentrum für Datenschutz (ULD), Germany

The remainder of this text is structured as follows: Section 2 describes the pilot trial applications of Privacy-ABCs as conducted in the ABC4Trust project. This information served as a basis for the discussions on application scenarios (elaborated in session I, see Section 3) and on legal and organizational issues with a focus on inspection and revocation (debated in sessions II and II, see Section 4). The conclusions are summarized in the final Section 5.

2 Privacy-ABCs in the Pilots of the ABC4Trust Project

The ABC4Trust workshop primarily addressed issues of Privacy-ABCs in practice. Therefore, starting point of the interactive discussions were the experiences gained from the pilots: In the ABC4Trust project privacy-preserving attribute-based credentials (Privacy-ABCs) were implemented in pilot trial applications to protect users' privacy. Privacy-ABCs provide options for attribute selection and attribute aggregation by the user. They can be used either fully anonymously or allow for conditional identification (so-called inspection) in order to support accountability. However, all these features can only be used to their best potential when they are implemented in a rights-centered way. The workflow of a Privacy-ABC authentication and Privacy-ABC features as well as their benefits are described in more detail elsewhere in this book (cf. [2]).

In the two pilots of the ABC4Trust project, Privacy-ABCs were used as means of authentication for an online communication platform of a Swedish school, where students, teachers and other stakeholders could securely and privately discuss matters of school life [3, 4, 5]. Some of the chat rooms were used fully anonymously, while in others a user's identity could be revealed under predefined conditions via an inspection process. In the other use case, the Greek University of Patras implemented an online platform for course evaluations [6, 7, 8]. There, students could rate their courses fully anonymously; the inspection feature was not implemented. However, in the second round of the pilot, students who participated in the course evaluation could obtain an additional credential which was inspectable. With this credential they could

enter a tombola and be selected to win a prize. In order to reveal the winning student's identity, the inspection process was implemented.

As with any authentication technology, there may be instances where the credentials issued through Privacy-ABCs have to be invalidated. In the ABC4Trust pilot trials this is for instance the case when a student leaves school or university. This can be realized through revocation of the respective credentials (for implementation in the pilots see [4] pp. 38 et sqq.; [7], pp. 18, 20; [8], pp. 77, 123).

Especially with regard to the school pilot, it is very clear that the inspection feature must not be used as a "backdoor" to reveal a user's identity at will. Instead, the full potential of Privacy-ABCs can only be achieved if inspection is an exception, rather than the rule. Similarly, a user loses all access to the respective service when her credentials are revoked. Therefore, revocation also has a users' rights dimension and should occur only in justified and limited instances. In order to safeguard this aim, a model process for inspection and guidelines for revocation were developed within the ABC4Trust project [9, 10].

3 Workshop Sessions on New Application Scenarios and Storage Devices

In session I, aspects of applying Privacy-ABC systems to new application scenarios were discussed based on the project partners' experiences with the project and from the pilots. Applying Privacy-ABCs to new application scenarios is not always a straight forward process, and despite being a technology with many features, Privacy-ABCs are sometimes not the most appropriate tool for a given scenario. Participants investigated potential new application scenarios (based on the scenarios tackled in sessions II and III). Moreover, they pondered how to validate whether Privacy-ABCs actually are the right tool for a given application, and – if so – how to map the entities of the scenario to the entities of Privacy-ABCs. Furthermore, the participants dealt with the process of developing policies and some related topics such as efficiency expectations etc.

As far as security tokens are concerned, the use of a storage device was suggested. In the workshop the participants assessed different options for tamper-proof devices (smartcards, mobile phones, USB sticks, etc.) which offer security and are ideal hardware tokens for storing the user's device key. The technical aspects for choosing a storage device as well as how the choice of the storage device could influence the user's confidence and trust to the system were explored. Also, it was found that the choice of the storage device could influence the usability of the system since the user has to carry the device with her every time she wants to use it.

Following up on this session, the participants had the opportunity to attend the additional hands-on session where they were tutored how to integrate ABC4Trust technology in future own applications. Instructions for developers as presented in these sessions are available at [11]. This encompasses the source code of the Privacy-preserving Attribute-based Credential Engine as well as further explanations on con-

cepts and features of Privacy-ABCs, the reference architecture, and the integration into an application.

4 Workshop Sessions on Inspection, Revocation, and Legal Issues

Two sessions tackled inspection and revocation, especially how to set up appropriate procedures with checks and balances: session II "Optional Features – Inspection and Revocation" and session III "Data Protection and Privacy Requirements for Privacy-ABCs". These sessions' primary goal was to improve and validate the model processes developed in the ABC4Trust project [9, 10].

4.1 Organization of the Sessions

In session II the focus lay on the inspection and revocation features of Privacy-ABCs as they have been implemented in practice within the Patras University pilot trial. Technical requirements and practical problems were explained in detail. The adaptability of the inspection and revocation tools to various needs and system as well as device requirements were demonstrated. From the practical experiences the responsible partners had gained with developing and piloting the application, guidelines for an optimal inspection and revocation process were given. This was illustrated with an in-depth look at the implementation of Privacy-ABCs in the ABC4Trust university pilot.

During session III participants were given an introduction to the European legal framework for data protection and privacy. This brief lecture addressed the bases in primary law for data protection legislation, including the fundamental rights to privacy and data protection. It focused on the obligations of data processors under the Data Protection Directive 95/46/EC and on data protection principles.

After this short presentation, participants were split into groups of four to five people. Based on their own knowledge and what had been taught in the beginning of the session, the participants' task was to assess one of five fictitious scenarios (see full descriptions in Appendix A), which dealt with a variety of existing and potential future Privacy-ABCs use cases. In each case, there were escalating levels of conflicts, which were to be resolved by finding an appropriate way of employing the inspection and revocation features.

In another step, the participants of the parallel sessions II and III joined. The scenarios, including their resolution by the participants of session III, as well as the model process for inspection [9] were discussed in the plenary. Participants of session II could comment on the findings from their practical background experience.

4.2 Discussions among the Participants

While each group was provided a different scenario description, similarities could be identified in the composition of the use cases: The group members were asked to act as if they were the people in charge of deciding on a conflict between various parties.

The objective was to think of measures to remedy the situation while achieving a balanced result. This may or may not mean to identify a Privacy-ABC user via inspection under specific circumstances; other measures also had to be contemplated. For deciding on a potential inspection, a list of inspection grounds was presented: Apart from possible internal policy demands as this was the case in the Swedish school pilot, these grounds covered:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- An existing court order or other valid administrative request because of criminal proceedings
- Damage compensation (protection of third people's rights claims)

The examples provided in the scenarios (cf. Appendix A) gradually escalated, e.g. from a conflict which could be remedied without the need for inspection (even if the anger shown may well be understandable in human terms) to a situation as severe as a threat to people's life. The fact that all examples contained the possibility of inspection did not mislead the participants into always choosing this instrument for achieving remedy. Interestingly enough, the legally trained persons among the groups did not dominate the discussions – it seemed that they did not have an advantage in answering the questions because they would have liked to first analyze all applicable national regulation which may have given further guidance. While that procedure is excellent for a thorough check of legal compliance, we focused in this exercise on the gut feeling of mainly laypeople, being no legal specialists.

4.3 Results

The discussions of the Summer School participants showed that they were very much aware of the privacy implications of revealing a user's identity through inspection. As the examples provided in the scenarios gradually escalated, every group adapted to each case by also escalating their responses. All of the groups found that in *variation 1* inspection was not a feasible option, as there were lower level solutions available, which were less invasive to the user's privacy (see Appendix A, "Situations to be discussed", no. 1). These included for instance deletion of offending posts in a forum. Additionally, the importance of properly defined inspection grounds was stressed, in order to facilitate the finding of a decision whether inspection even was an option.

In *variation 2* (see Appendix A, "Situations to be discussed", no. 2), the participants had to weigh the conflicting interests and rights of the user and the service provider to reach a nuanced solution for the problem. With respect to this balancing exercise, participants stressed the importance of the separation between the entity performing the weighing and the entity to reveal the identity. Ideally, the entity deciding on a solution should consist of all relevant stakeholders in the use case, i.e. not only representatives of the service provider, but also users. Additionally, it is desirable to incorporate an element of external supervision to this decision entity, in the form of an external expert focused on ethical or legal implications of the decision. It was further discussed that the service provider's Data Protection Officer could partake in the

deliberations, as he or she is an expert with a certain level of autonomy. Alternatively the Data Protection Officer could be involved in reviewing and auditing the process. This review is enabled by an audit trail that logs any activity within the process on all its stages, comprising e.g. technical access log entries as well as manually generated reasoning for inspection decisions. This could be supported by an automated ticketing system, which can provide check lists and assist the various entities in the execution of the process.

When participants were asked to outline a model for an inspection process, almost all of the groups suggested that this entity should be independent from the service provider in finding a solution for a problem.

As *variation 3* (see Appendix A, "Situations to be discussed", no. 3) included instances of emergencies, such as threats to the life or physical integrity of persons, participants agreed that there was a need to ensure a quick response, which can be realized through break glass procedures. This could include fast-tracking decisions of the entity deciding whether an inspection should take place. However, as the levels of emergency in the various scenarios differed to an extent, the concept of what constitutes an emergency was discussed controversially. It was concluded that just as the inspection grounds themselves emergency situations should be clearly defined in advance in order to use the full potential of Privacy-ABCs.

The additional questions in some of the scenarios, e.g. concerning the timing for proving that a customer in an e-commerce setting is over 18, stimulated further discussions in the individual groups. In the case of ordering alcohol or cigarettes it was discussed that the proof would be necessary only at check-out time, but the customers should be made aware of such requirements from the beginning. If adult content may not even be displayed to customers younger than 18, proof would be required before showing the content, similar to realizing a separated room with special access control.

4.4 The Model Inspection Process

In the group discussions a few ideas emerged on a structured workflow, defined entities, and assigned tasks for the inspection process, and similarly for any unplanned revocation. While many papers on inspection only focus on technical issues such as the process of decrypting inspectable tokens by an entity (i.e. the *Inspector*) that has access to the inspection key, the organizational and legal setting would be relevant, too. For this purpose, a model inspection process was developed [9, 10] that contains several roles and looks a bit more complex than simply adding the *Inspector* component (see Fig. 1). However, it is de facto quite similar to other workflows where a service provider is notified about a conflict and has to react accordingly. Also, it is important to understand that inspection should be the exception rather than the rule. This is the reason for separating the access to the inspection key and to the encrypted inspectable tokens as long as no inspection has to be performed.

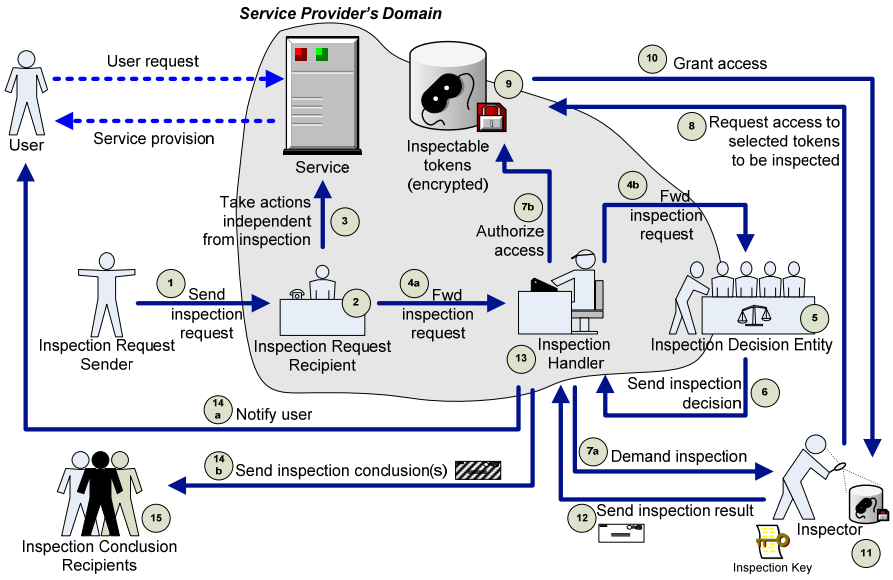

Fig. 1. A model inspection process [9]

The process starts with an inspection request, sent by the *Inspection Request Sender* to the *Inspection Request Recipient* within the *Service Provider's Domain* (step 1). This could be a user who thinks a policy rule has been violated, or it could be the police demanding inspection in an investigation, potentially with a warrant issued by the competent judicial authorities. The *Inspection Request Recipient* has to check the inspection request (step 2). In some cases, actions independent from inspection could be taken (step 3), e.g. removal of an insulting posting. Note that such an intervention could mean an infringement of users' rights and needs a balancing approach, too.

The *Inspection Request Recipient* forwards the inspection request to the *Inspection Handler* (step 4a) where the entire inspection process is being orchestrated. The first action of the *Inspection Handler* is a further forwarding of the inspection request to the *Inspection Decision Entity* (step 4b). This could be a board of different stakeholders where difficult conflicts may be discussed to achieve a balanced solution. The decision on whether to inspect or not (step 5) is documented and sent back to the *Inspection Handler* (step 6).

In case inspection should be performed, the *Inspection Handler* orders the *Inspector* to inspect specific inspectable tokens (step 7a) and authorizes access for the *Inspector* to those tokens stored within the *Service Provider's Domain* (step 7b). The *Inspector* requests access to selected tokens to be inspected (step 8). This request is checked against the authorization (step 9). In case of a match access is granted (step 10), otherwise this attempted access would be logged, and the process would end.

The *Inspector* who possesses the inspection key decrypts the tokens (step 11) and sends the inspection results to the *Inspection Handler* (step 12). The *Inspection Handler* takes action based on the inspection results, e.g. notifying the *User* whose identi-

ty has been revealed (step 14a), generating target-specific inspection conclusions, and informing the *Inspection Conclusion Recipient(s)* (step 14b). This recipient could be identical with the *Inspection Request Sender*, but may also be different. Again, further steps may be taken by the *Inspection Conclusion Recipients* (step 15).

Further details, e.g. on the legal relation between *Inspector* and *Service Provider*, on the composition and tasks of *Inspection Decision Entity*, on demanded logging of decisions for accountability purposes, and on possible short cuts in the process (e.g. in case of a valid warrant that has to be obeyed, or in cases of emergency), have been discussed in [9]. Looking at the model process, the participants of the session developed ideas on splitting the inspection key between the *Inspector* and the *Inspection Decision Entity*. Moreover, they discussed possible consequences in case the *Service Provider* and the *Inspector* reside in different jurisdictions and governmental access to the key or to the data is demanded.

5 Conclusions

The ABC4Trust workshop was characterized by vivid discussions with and among the Summer School participants and led to a much appreciated input. In the technical sessions new application possibilities were identified. The practicability and usefulness of the information provided online for developers, together with source code [11], could be tested. The feedback of the participants was valuable for improving the developers' material.

The two other sessions on balanced procedures for inspection and revocation showed a broad acceptance of the model process developed in the ABC4Trust project. The general patterns of the interaction between participants, who had not been familiar with the model inspection process before, confirmed that the processes developed for inspection and revocation flow from the operationalization of a privacy- and user rights-centered approach. Participants generally concluded that specific implementations have their own factual and legal requirements and thus implementation always has to be use case specific. Nevertheless, the model inspection process as it was presented to the participants after the discussions was appraised as a way to enhance transparency and make the best use of the privacy-friendly technology employed in the ABC4Trust project pilots.

A Appendix

This appendix contains the five scenario descriptions that were handed out to the participants of the workshop. Each group had to assess one of the scenarios (school, e-commerce, casino, car rental, e-petitions) and think of solutions for different escalating situations.

School Scenario. *Task:* You are the people in charge of deciding on the case detailed below. Which measures can you adopt to remedy the situation while achieving a balanced result? How can this process of revealing a user's identity best be implemented in practice to ensure a system of checks and balances?

The *N School* runs a Privacy-ABC based communication system. All pupils of the school can use the communication system, inter alia for chatting with each other, sharing documents and seeking advice from the school's counsellors. The pupils act under pseudonyms they can choose anew any time.

Inspection grounds:

To guarantee the physical and mental safety of each participating pupil, the School Communication System foresees in all restricted areas except those for political discussions the revelation of the pupil's identity (called inspection) in certain predefined emergency situations (called inspection grounds).

Inspection grounds:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- Situations demanding an intervention according to the school policy against discrimination and degrading treatment. It strives to prevent discrimination based on gender, sexual orientation, ethnic background, religion. The policy also sanctions harassment and other threats to the safety of students, including offensive language. It is a legal requirement to report such behavior and the names of the perpetrators to the school authority.
- An existing court order or other valid administrative request
- Damage compensation (protection of third people's rights claims)

Class 9b has opened a chat room "9B Only", their own restricted area, accessible only to pupils and teachers of class 9b. The class and its teachers use this chat room especially for exchanging information on class activities – for instance a boat trip to the small rock islands along the shoreline.

Situations to be discussed:

1. The boat trip was fun. The pupils took hundreds of photos. *Pupil A* shares several photos she took in the restricted area of class 9b. One of the photos is a portrait picture of *B*. *B* is not happy with the photo visible for the whole class. She recently has decided to be a punk and therefore dyed her hair green. But on the picture, tak-

en two days ago, she is still naturally blonde. She demands deletion, first via chat and then in front of the class. *A* thinks that *B* has simply gone bonkers and decides neither to say that it was her who uploaded the picture nor to delete it. *B* thinks she has the right to deletion of the picture and to know who uploaded it. She demands inspection. She wants to confront the "photographer" personally.

2. Finally, *B* found out that it was *A* who uploaded the picture. She is extremely disappointed, since she had thought A was her friend. *B* writes a chat message to all: "I never thought *A* would not respect other people's feelings. I think everyone has the right to express her own personality. I am very disappointed that *A* did not delete the picture. I am not her friend anymore." *A* feels offended – she is sure that it was *B* who wrote this. Since she is kind of clever, she decides not to answer in a way that would identify her as *A*. She writes: "I think what *A* did was alright. *B* is always exaggerating – she is such a wannabe and a drama queen and just silly." A lively discussion is initiated. *X1*, *X2*, and *X3* agree with what *A* wrote and call *B* "birdbrained", "dumb blonde" and "insane".
3. *B* is devastated. No one understands her or even seems to take her seriously. Furthermore, everyone is making fun of her because of her new style. Former friends seem to stay away from her. So, late at night, after a day full of frustration, *B* writes the following chat message to "9B Only": "I will kill you all. I got a reason, I got the means – tomorrow I will use the opportunity!"

E-Commerce Scenario. *Task:* You are the people in charge of deciding on the case detailed below. Which measures can you adopt to remedy the situation while achieving a balanced result? How can this process of revealing a user's identity best be implemented in practice to ensure a system of checks and balances?

The e-commerce platform *E-Buy* offers traders to sell their goods via its portal. It is based on Privacy-ABC technologies. Users/potential customers do not reveal their identity to *E-Buy* nor to the sellers when registering to *E-Buy* and going shopping. They act under pseudonyms they can choose anew any time. Users can also rate the products they bought. The rating is visible to everyone who visits the platform. A user can have her products delivered to a central store, and pick them up there by identifying herself using the credential she gets from *E-Buy* when buying the respective products.

Customer C is looking for a mosquito blind. He makes a find among the products provided by *D* who mainly sells pesticides and other means to control pests. *C* buys the mosquito blind. When unpacking the mosquito blind, *C* finds a manual how to fix the mosquito blind on windows. One has to cut it to the proper size. *C* reads the manual carefully. But, however, he comes to the conclusion that one has to measure the internal side of the window's frame. In fact, one has to measure the outer dimensions. Consequently, the mosquito blind is too small for the window and *C* cannot make use of it like this. *C* tries to call the seller *D*. *D* just says the product and manual were fine.

Inspection grounds:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- An existing court order or other valid administrative request because of criminal proceedings
- Damage compensation (protection of third people's rights claims)

Situations to be discussed:

1. *C* feels his problems were treated as a joke or something. He is angry and rates the mosquito blind with only one of five possible stars. Additionally he states, "In my opinion, the instruction manual provided by the seller was inadequate. Like this it is de facto impossible to fix this mosquito blind. The manual clearly states that in order to find the right size one has to measure the internal side of the window's frame. In fact, one has to measure the outer dimensions. Otherwise the mosquito blind is too small." *D* does not want this comment to ruin his impeccable reputation. In fact, he does not sell any mosquito blind during the following week. *D* is convinced that *C*'s rating irritates other customers. He demands the revelation of this customer's identity, in order to claim compensation from *C*.
2. *C* is furious. His rating of *D* is gone! Fortunately *D* still sells goods on *E-Buy*. *C* picks a nice rat trap. Actually *C* just wanted to have another possibility to rate *D* on *E-Buy*. So, after the trap was delivered, *C* writes, "No rat trap is big enough to trap the biggest rat on *E-Buy*: Its seller. *D* is a fraudster and sells inferior crap." *D* thinks this is a severe offence and wants to make a complaint.
3. Alternative: *C* is really furious. His rating is gone. Fortunately *D* still sells goods on *E-Buy*. *C* picks some poisonous gas (meant to be used for parasite prevention). After the gas was delivered, *C* writes, "Caution you pest! I got the gas and I know where you live. You will not live through this night!"
4. Additional question: On the *E-Buy* platform some traders sell alcohol and cigarettes. According to the self-imposed rules of *E-Buy* such products may not be sold to persons under age 18. At which point should the potential customer have to prove that she is over 18?

Casino Scenario. *Task:* You are the people in charge of deciding on the case detailed below. Which measures can you adopt to remedy the situation while achieving a balanced result? How can this process of revealing a user's identity best be implemented in practice to ensure a system of checks and balances?

J has is addicted to gambling. Since *J* is a junkie, but has a sense of style he only visits casinos of the *LB Group*. Admission only to members. *LB* casinos have a Privacy-ABC based access control system. This means, members can prove their membership (and access permission) via their smartphones when entering the casinos. The membership credentials also contain information about how much money is stored on a member's account, since one cannot pay in cash at *LB* casinos. The *LB Group* only

learns that a member has entered one of their casinos, but not which member. It cannot analyze the member's usage behavior.

In the past five years, it got worse and worse. *J* lost his friends, because he borrowed money from them and never gave it back and lost his job because he repeatedly was gone for days without permission. Finally, his girlfriend threatens to move out if *J* does not stop gambling, because she cannot stand it anymore. Sitting on his mount of debt – round about EUR 250,000 – *J* comes to the conclusion that something has to change.

Inspection grounds:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- An existing court order or other valid administrative request because of criminal proceedings
- Damage compensation (protection of third people's rights claims)

Situations to be discussed:

1. Via the Privacy-ABC based *LB* communication system for members, *J* resigns his *LB* casino membership contract. *LB Group* accepts the notice, but denies releasing *J* from the membership contract immediately. It insists on the notice period of 3 months. *J* is devastated. Once committed to get rid of his gambling addiction by just keeping himself from going to the casino, he wants to make sure that he cannot access *LB* casinos anymore. Even though for the next 3 months he still will be a member. His girlfriend does not believe him that he will not go to the casino anymore although he still could.
2. Although *J* managed not to gamble anymore for 4 weeks, his girlfriend left him for a professional poker player. *J* does not see any reason why he should not start gambling again. He wants to have access to the *LB* casinos again. In the end, he might still make a fortune … The *LB Group* is very generous and accepts the withdrawal of the notice. *J* will stay a member. But his membership credential is not valid anymore. He does not want a whole new membership credential, because there is still money stored on his original one.
3. Believe it or not – *J* won 2 million Euros in one night. Boosted by such a success, *J* visits several *LB* casinos in the following days. Now that he is rich he can travel. And he keeps winning. The *LB Group* – due to Privacy-ABCs – does not know that it is always the same member who is winning tons of money. But the management is suspicious. In statistics, this is more than the standard deviation. *LB Group's* lawyers suspect fraud. All the money is won in Black Jack. *LB Group* wants to know if it is the same person who is winning all the time.

Car Rental Scenario. *Task:* You are the people in charge of deciding on the case detailed below. Which measures can you adopt to remedy the situation while achiev-

ing a balanced result? How can this process of revealing a user's identity best be implemented in practice to ensure a system of checks and balances?

Ride Ltd. runs a conventional car rental via an online platform. The platform is Privacy-ABC based. Users do not reveal their identity to *Ride Ltd.* when registering to the platform and renting cars. They act under pseudonyms they can choose anew any time. Users can pick up the car keys and the car from a central parking lot by identifying themselves using the credential they get from *Ride Ltd.* when renting a car. *Ride Ltd.* terms and conditions of business determine that in case of damages up to an amount of EUR 100, it is entitled to just debit the amount from the customer's account. Such damages include minor accident damages, reimbursement of costs related to inappropriate use of the car, and giving back the car in a non-contractual condition. Customers are required to give back the car refueled.

N rents a car for a nice weekend trip to the sea side.

Inspection grounds:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- An existing court order or other valid administrative request because of criminal proceedings
- Damage compensation (protection of third people's rights claims)

Situations to be discussed:

1. *N* is back from the seaside. It has been a long day and he just wants to go home. The tank is really empty and *N* hardly makes it to the parking lot. Whatever – *N* just parks the car on the parking lot of *Ride Ltd.* and places the keys in the letterbox. The next morning, *E* – an employee of *Ride Ltd.* – checks the car and finds the empty tank. He cannot even drive the car to the gas station. *E* has to haul the gasoline canister to the car … thank you very much, dear customer …
2. After refueling the car, *E* checks the interior. What the …? The whole backseat is full of blood. Indeed, *N* went fishing and made a pretty good catch. Unfortunately, the fish obviously had not had properly bled when *N* threw it on the back seat. Put briefly, the back seat is ruined and cannot be cleaned. The replacement will cost about EUR 3,000. *Ride Ltd.* contacts the customer – *N* – but of course *Ride Ltd.* only knows the pseudonym of the customer who had rented the car via the internal communication system. *N* does not answer. *Ride Ltd.* wants to claim compensation from him.
3. While the lawyers of *Ride Ltd.* are preparing the civil proceedings against *N*, there is an incoming call. It is the police. A witness alleges that a man has just forced a girl into a car of *Ride Ltd.* The police suspect a crime – kidnapping or abduction – and want to know who has currently rented the car.

E-Petitions Scenario. *Task:* You are the people in charge of deciding on the case detailed below. Which measures can you adopt to remedy the situation while achiev-

ing a balanced result? How can this process of revealing a user's identity best be implemented in practice to ensure a system of checks and balances?

In country *X* everyone has the right to petition to the parliament. It is a fundamental right which guarantees that the public authorities at least have to file the petition. If the public authority lacks competence concerning a petition's content, it may dismiss the petition as inadmissible. Within the parliament there is a petition committee which is competent to decide on and answer petitions. Petitions offer the possibility to raise an issue and oblige the democratically elected representatives to address this issue. They can be filed in writing (via post) or electronically, via an online form which is provided on the petition committee's website. The website employs Privacy-ABCs. This means, users can petition anonymously. Petitions are published automatically online if the petitioner does not object when filing the petition. Since the petitions are not manually checked before they are published online, you sometimes find interesting howlers inside …

Inspection grounds:

- Situations implying a severe threat to the life, or the physical/mental integrity of a person
- An existing court order or other valid administrative request because of criminal proceedings
- Damage compensation (protection of third people's rights claims)

Situations to be discussed:

1. "After almost 10 years of female rule of *President M* we are only inches away from the abyss. Everything will run down the drain if we do not stop them. We need to take a step back, back to the days when the world was still governed by worthy men – and only by men. Reasonable, reliable, and down-to-earth. Women are nothing but a victim of their genes and hormones. We cannot let them govern our homeland any longer. Abolish women's suffrage!!!"
2. "The killing of male chicks is a blatant injustice which cannot be accepted anymore! We, the *National Chicken Liberation Forces*, demand satisfaction! The killing must be stopped immediately. If the parliament does not adopt an anti-male-chicken-killing law within the next 48 hours, we will free all chicken farms!"
3. In country *X* all armament deals are subject to the approval of a supervisory board. In general, weapons from *X* may not be sold and delivered to countries which are currently considered as "region in crisis". *Y* owns an arms company. Business is going pretty bad since, due to all those crises in the world, the supervisory board does not easily give the green light to all deals anymore. *Y* panics a bit. So he petitions the parliament: "If you do not drop the prior approval, I will give you a product presentation right in the middle of the parliament! Our tanks will break your walls and make you approve them!"
4. Additional question: Assumed, someone is petitioning all the time – say, twice a day. What to do?

References

1. Rannenberg, K., Camenisch, J., Sabouri, A. (eds.): Attribute-based Credentials for Trust – Identity in the Information Society. Springer, Heidelberg (2015).
2. Sabouri, A., Rannenberg, K.: ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-life. In: Proceedings of IFIP Summer School 2014 (this book), Springer, Heidelberg (to appear in 2015).
3. Bcheri, S., Goetze, N., Orski, M., Zwingelberg, H.: Application Description for the School Deployment. Deliverable D6.1 of the ABC4Trust Project (2012), `https://abc4trust.eu/download/ABC4Trust-D6.1-Application-Description-School.pdf` (accessed 22 March, 2015).
4. Abendroth, J., Bcheri, S., Damgaard K., Ghani, H., Luna, J., Mikkelsen, G.L., Moneta, M., Orski, M., Suri, N., Zwingelberg, H.: Necessary Hardware and Software Package for the School Pilot Deployment. Deliverable D6.2 of the ABC4Trust project (2013), `https://abc4trust.eu/download/ABC4Trust-D6.2.Hard-and-Software-Package-for-School-Pilot.pdf` (accessed 22 March, 2015).
5. Bcheri, S., Björk, E., Deibler, D., Hånell, G., Lerch, J., Moneta, M., Orski, M., Schlehahn, E., Tesfay, W.: Evaluation of the School Pilot. Deliverable D6.3 of the ABC4Trust Project (2014), `https://abc4trust.eu/download/Deliverable%20D6.3.pdf` (accessed 22 March, 2015).
6. Abendroth, J., Liagkou, V., Pyrgelis, A., Raptopoulos, C., Sabouri, A., Schlehahn, E., Stamatiou, Y., Zwingelberg, H.: Application Description for Students. Deliverable D7.1 of the ABC4Trust project (2012), `https://abc4trust.eu/download/ABC4Trust-D7.1-Application-Description-Students.pdf` (accessed 22 March, 2015).
7. Damgaard, K, Ghani, H., Goetze, N., Lehmann, A., Liagkou, V., Luna, J., Mikkelsen, G.L., Pyrgelis, A., Stamatiou, Y.: Necessary Hardware and Software Package for the Student Pilot Deployment. Deliverable D7.2 of the ABC4Trust project (2012), `https://abc4trust.eu/download/ABC4Trust-D7.2.Hard-and-Software-Package-for-Student-Pilot.pdf` (accessed 22 March, 2015).
8. Deibler, D., Engeler, M., Krontiris, I., Liagkou, V., Pyrgelis, A., Schlehahn, E., Stamatiou, Y., Tesfay, W., Zwingelberg, H.: Evaluation of the Student Pilot. Deliverable D7.3 of the ABC4Trust Project (2014), `https://abc4trust.eu/download/Deliverable%20D7.3.pdf` (accessed 22 March, 2015).
9. Bieker, F., Hansen, M., Zwingelberg, H.: Towards a Privacy-Preserving Inspection Process for Authentication Solutions with Conditional Identification. In: Hühnlein, D., Roßnagel, H. (eds.): Proc. Open Identity Summit 2014. Lecture Notes in Informatics, vol. P-237, pp. 85-96. Gesellschaft für Informatik, Bonn (2014).
10. Bieker, F., Hansen, M.: Modelling the Inspection Process/Considerations Concerning the Revocation Process. In: Rannenberg, K., Camenisch, J., Sabouri, A. (eds.): Attribute-based Credentials for Trust – Identity in the Information Society, pp. 155-161. Springer, Heidelberg (2015).
11. Alexandra Institute, Miracle, and IBM Research – Zurich: Privacy-Preserving Attribute-Based Credential Engine (p2abcengine). Repository on GitHub (2015), `https://github.com/p2abcengine/p2abcengine` (accessed 22 March, 2015).