Extensions to the Privacy-preserving Identity Card (Extended Abstract)

Yves Deswarte[1,2], Sébastien Gambs[1,2]

[1] CNRS ; LAAS ; 7 avenue du Colonel Roche, F-31077 Toulouse, France
[2] Université de Toulouse ; UPS, INSA, INP, ISAE ; LAAS ; F-31077 Toulouse, France
{Yves.Deswarte,Sebastien.Gambs}@laas.fr

1 Privacy-preserving Identity Card

Recently, we have proposed to replace the national identity card, currently used in many countries, by a personal device that allows its user to prove some binary statements about himself while minimizing personal information leakage [2]. We call this device a *Privacy-preserving Identity Card* (PIC) because contrary to the identity cards currently deployed, it is designed to respect both the principles of *data minimization*[1] and *data sovereignty*[2].

The privacy of the user of a PIC is protected through the use of anonymous credentials which allows him to prove binary statements about himself to another entity without having to disclose his identity or any unnecessary information. The proposed scheme also prevents the possibility of tracing the user, even if he proves several times the same statement (unlinkability property). A tamper-proof smartcard is used to store the personal information of the user thus protecting his privacy and preventing the risks of forgery at the same time. The user identifies himself to the card via biometrics thus forbidding an unauthorized use in the situation where the card is stolen or lost. When the smartcard is inserted into a reader device, the smartcard processor initiates a mutual authentication between the card and the reader. This phase involves using a simple signature scheme and a group signature scheme. First, the reader proves to the card that it is an authentic reader by showing that is possesses a valid credential signed by the certification authority. The questions that the reader is allowed to ask he card is also part of this credential as well as the public encryption key of the reader. Then, the card proves to the reader that it is an authentic card by

[1] The data minimization principle states that only the information necessary to complete a particular application should be disclosed (and no more). This principle is a direct application of the legitimacy criteria defined by the European data protection directive (Article 7, [3]).

[2] The data sovereignty principle states that the data related to an individual belong to him and that he should stay in control of how these data are used and for which purpose. This principle can be seen as an extension of many national legislations on medical data that consider that a patient record belongs to the patient, and not to the doctor that creates or updates it, nor to the hospital that stores it.

showing that it belongs to the group of valid smartcards/users, more precisely, by signing a random challenge issued by the reader with its private group signature key. Afterwards, the card will enter a question-response protocol with the reader, where its answers can be for instance in the form of non-interactive zero knowledge proof of a particular statement corresponding to the question asked by the reader[3] and will be encrypted using the public key of the reader so that only it can decrypt them.

Consider for instance the following scenario that illustrates how such a card would work in practice.

Scenario 1 (Alice in Anonymityland) *Alice is privacy addicted since she has read the seminal paper of Chaum on anonymity [1]. She has recently seen in an advertisement that her government now offers the possibility of using a privacy-preserving identity card. Therefore, she goes to the town hall and asks for it. The city hall checks the validity of Alice's identity, scans her biometric data and sends them in a secure manner (for instance using a protected conveyor) along with her personal information to the corresponding governmental service that will be responsible for issuing the card.*

For an external observer, the card looks exactly the same as any other privacy-preserving identity card, since there is no personal information written on the plastic card. Effectively, the card is a tamper-proof smartcard containing anonymous credentials that Alice can use to prove some statements about her. The card is activated by Alice's biometric features. For instance, her card allows Alice to prove her nationality when she crosses the border, to show that she is within some age interval in order to gain some discount at the theater, to certify her identity when she takes the plane or to gain access to local services restricted to her neighborhood residents.

If the card of Alice is lost or stolen, she does not need to worry about its misuse for malicious purpose, thanks the biometrics authentication and the tamper-proof features of the smartcard. Instead, she simply returns to the city hall to declare the loss of her card and ask for a fresh privacy-preserving identity card.

Ideally and independently of the technologies used, we think that any implementation of the PIC should fulfill the following properties:

- *No personal information leakage*: in order to protect the privacy of the user, the card should disclose as little information as possible about him (ideally only one bit of information).
- *Unlinkability*: it should not possible to trace and link the actions of the user of the card, even he proves the same statement at different occasions to the same entity.
- *Ownership proof*: only the legitimate user should be entitled to use his PIC to prove statements about himself to other entities. This means that some authentication mechanism has to take place between the user and the card.

[3] Other implementations of the privacy-preserving proof of statements are possible.

– *Authenticity*: some mutual authentication has to be performed between the card and the reader device in order to prevent the possibility of an adversary impersonating the role of a valid PIC or a valid reader.
– *Correctness*: a binary statement proven by the user with the help of the PIC should always be valid. For instance, the user should never be able to prove false statements about himself by cheating the system (*soundness property*). Moreover if the reader is honest, it should always accept a binary statement about the user provided that this statement is true and the user possesses the corresponding credentials (*completeness property*).
– *Unforgeability*: in order to avoid someone counterfeiting the identity card, the card should be tamper-proof and have an inherent ability to resist hardware and logical attacks.

Apart from these fundamental requirements, the PIC may also respect some additional properties such as:

– *Optional anonymity removing*: the actions of the user should stay anonymous at all times, except in some scenarios where it might be necessary to remove his anonymity for serious reasons. For instance in an extreme situation, it could happen that a crime (such as a murder) has been perpetrated in a room that has been accessed by only one person using a privacy-preserving identity card. In this situation, the reader and the certification authority may want to collaborate in order to lift the anonymity of this person. On the other hand, although the possibility of lifting the anonymity is desirable in some scenarios, it could also decrease the confidence of the user in his belief that his privacy will really be protected by the card.
– *Explicit consent*: in order to increase the trust of the user in the system, the card could monitor the questions that it has been asked and display them to the user. It is even possible to imagine, that for some questions that are deemed critical regarding the privacy of the user, his confirmation may be asked before the privacy-preserving identity card replies to the question.

2 Extensions to the Privacy-preserving Identity Card

Originally, the main purpose of the PIC is to enable a person to conduct tasks in the real world without having to disclose his identity but the same device could potentially be used to access to online services such as e-government services or even e-business applications. We list here some possible extensions to the original concept of PIC:

– *Access to e-government services.* In case of online access to e-government services, the card could be plugged to a standard personal computer via an external trusted USB reader certified by the government. The e-government services could include for instance the online declaration of income, the consultation of the user's file as recorded in the database of a certain ministry or printing some official documents related to the identity of the user. In

this case, all the communication between the reader and the e-government platform hosting the online services should be encrypted to prevent potential information leakage, e.g., to a spyware that would have infected the user's personal computer.

- *Access to e-business applications.* Another online extension would be to use the PIC as an authentication mean during access to e-business applications. For instance, when paying a purchase on Internet, the PIC could be used to show that the current owner of the credit card used for the payment is also the current owner of the PIC. Using a system of anonymous credentials, it would be possible for the user to prove this statement anonymously (i.e., without having to disclose explicitly his identity to the e-business server). Of course, in this virtual context it may be more difficult for a user to keep an explicit control on how his data are used and we may have to cope with more threats than in the simple card-reader interaction scenario presented in the previous section. For instance, we could imagine some kind of phishing attack where the user receives an email making some advertisement for a particular online store together with an associated website address. If he is the malicious owner of this website, a malicious adversary could sit on the link between the card and the server and performs a man-in-the-middle attack. More precisely, the adversary would pretend to be a genuine online store to the card and relay the answers provided by the card to the real store and vice-versa and thus gain access to resources in the behalf of the owner of the PIC (imagine for instance that the adversary makes the user of the PIC pay for the tunes he downloaded from an online music store). Note that the same kind of attack may also apply for the access to e-government services in which case it could lead to a privacy breach where the adversary learns personal information related to the user of the PIC (which could be used later for fraudulent ends such as identity theft).
- *E-voting.* Consider also the scenario where the card is used for authentication during an election where it is possible to vote electronically. One can imagine a protocol where the user can prove his right to vote in a privacy-preserving manner using the PIC and such that he can cast only one vote. However, even if this application protects the identity of the voter and his choice, it does not address the usual threat of coercion, which is a recurrent problem of the e-voting setting. Someone could for instance point a gun at you when you are voting from your home or buy your vote and ask to be there as a witness when you cast your vote online.
- *Integration within a cell phone.* Another possible extension to the privacy-preserving identity card is to embed it directly in a device such as a cellular phone. Of course, this raises the question of how much trust can be put in such a device. Indeed, the user has to trust that his cell phone will only access his PIC in a rightful way and will not try to collect information about him, e.g., by recording the questions and their answers. Normally the answers of the PIC are encrypted at the beginning of the chain (in the PIC itself) and not accessible to the phone, however in some situations it is possible to deduce them indirectly, for instance if the user gain access to a resource

such as a file after his interaction with an online service. Moreover, simply registering the questions can be used to trace the actions of the user (for instance if he often tries to have a discount when going to his neighborhood swimming pool) and thus constitute a form of profiling. To trust that a cell-phone is perfectly secure may be more demanding than trusting that a PIC and a reader (which have been certified by the government or an independent authority) are genuine. One of the advantage of using a cell-phone is that it can provide the contactless facilities but without the risk of the usual contactless smartcards which can be skimmed without even the user noticing it. The PIC may also use the computational and memory capacities of the phone to its own benefit. For instance, the phone may add another level of encryption to the output of the PIC or register questions asked so far to the PIC and refuse to pass a question to the card when it decides that this question may endanger the privacy of the user (which is a form of profiling, but this time for the benefit of the user's privacy).

- *Use as an electronic wallet.* Another extension is to use the PIC as an electronic wallet by drawing on techniques such as one-time anonymous credentials. In such a scenario, the content of the card could be updated regularly via a certified terminal. The one-time credentials can play the role of electronic cash but also be used as e-ticket. For instance, when Alice buys a ticket concert from a vending machine she could upload the corresponding one-time credential on her privacy-preserving identity card while paying with anonymous e-cash. Later, the one-time credential of her ticket could be transmitted at the entrance of the concert hall via Alice's cellphone. Another application may include buying electronic tokens to access the transport system.
- *Integration of biometric sensor and display screen within the card.* If the card integrates directly a biometric sensor and a display screen, this can greatly enhance the trust of the user regarding the PIC as he does not need to trust anymore another apparatus such as an external biometric sensor or the screen of the reader or of his cell phone. Indeed, if embedded within the PIC, the biometric sensor can communicate directly with the smartcard thus limiting the risk of someone eavesdropping the communication channel. Moreover, it makes it more difficult for an adversary to acquire the biometric data of the user as the biometric sensor is directly in the hands of the user himself. The screen can be used to display the questions asked to the card but also its answers. Suppose for instance that the current user needs to prove that he is the owner of a particular PIC and that when he puts his fingerprints on the biometric reader his face is displayed on the screen of the card. This does not give any new information except that the current user is also the owner of the card (unless the card has been tampered with).

Such extensions would require an in-depth security analysis to ensure that they can be safely integrated in a privacy-preserving identity card but it is technically feasible to develop and deploy such an extended privacy-preserving identity card with currently available technologies. One fundamental question is whether or not developing a identity card achieving many functionalities differing

from its original purpose (as it is currently the trend in many countries) is really a good idea at all. Indeed, it constitutes a *single point of failure* that if compromised will have serious consequences including a major impact on the privacy of the user.

References

1. D. Chaum, "Security without identification: transaction systems to make Big Brother obsolete", *Communications of the ACM* **28**(10), pp. 1030–1044, 1985.
2. Deswarte, Y. and Gambs, S., "Towards a privacy-preserving national identity card", *LAAS Report 09208, submitted for publication*, 2009.
3. European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995* on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML`.