A Survey on Untransferable Anonymous Credentials
extended abstract

Sebastian Pape
Databases and Interactive Systems Research Group, University of Kassel

Abstract. There are at least two principal approaches to prevent users from sharing their anonymous credentials: adding valuable secrets into the system the user does not want to share or embedding biometric access control. This work aims to identify possible fields of application and compare both approaches in respect of the credentials’ untransferability.

1 Introduction

Anonymous credentials introduced by Chaum [1, 2] usually consist of cryptographic tokens which allow the user to prove a statement or relationship with an organisation to another person or organisation anonymously. While anonymous credential systems are related to the concept of untraceable or anonymous payments [3] and hence credentials can be easily transferred to another person, there are some situations where transferring a credentials is undesired. E.g. people who have to prove their age to an organisation if they want to buy alcoholic drinks or tobacco or if they want to visit a bar or discotheque. If the organisation is not trustworthy to the user, he probably does not want to disclose more information than “I’m 18 or older”. Analogous circumstances apply during online age verification, where it is common to show credit card information to prove a certain age. Since the user does not know if the age verification site is trustworthy, he does not want to give this data away. On the other hand, the organisation demands a proof of age of the specific user and not of his relatives or friends, which would rather prove the statement “I know someone who is 18 or older.”. Other examples of the utilisation of anonymous credentials could be the proof of a country’s citizenship, driving licenses or the proof of special abilities such as academic degrees.

There are two well-known approaches to prevent users from sharing their credentials. One approach to prevent the transfer of credentials is to equate sharing a credential with sharing a valuable secret outside the system [4] or even all of the user’s secrets inside the system, namely credentials from other issuers [5]. Another possibility of assuring untransferability of anonymous credentials is to make use of biometric control devices [6]. Of course, care has to be taken that these devices do not break the user’s anonymity.

This work aims to elaborate on the advantages and disadvantages of both approaches with regard to the untransferability of credentials. The outline of this
The next section describes anonymous credentials and possible implementations, while Section 3 introduces our scenario and attacker model. Section 4 investigates the approaches’ untransferability and eventually we end with conclusions in Section 5.

2 Anonymous Credentials

The basic idea of anonymous credentials is that users are able to prove attributes issued by an organisation anonymously. Implementations usually access proofs of knowledge in combination with blind signature [7] and group signature [8] schemes.

This is only one authentication factor “knowledge”, but it can easily be transformed to “possession” by moving the secret into a smartcard, where we presume it cannot be reached. The smartcard then works as a blackbox for the user and if he does not trust the manufacturer of the card or the issuing organisation, we assume the user carefully observes the communication of the card with the verifier following Chaum’s and Pedersen’s wallet with observer architecture [9].

This concept suggests each user has a personal communication device (called wallet) with a tamper-resistant chip (called observer) either built-in or in the form of a smartcard. Now the user is able to check and prevent information flow from the organisation to the observer and only has to trust that the observer supports all legitimate operations. The verifying organisation on the other hand only has to trust that the observer is still intact and prevents illegitimate operations (e.g., releasing the secret). To prevent abuse the tamper-resistant chip may be protected by a PIN resulting in a two-factor-authentication (possession of card and knowledge of the PIN) as already known from today’s cash cards.

Embedded Valuable Secrets. The idea of this approach is to discourage the users from sharing their credentials by equating the sharing of their credential with sharing a valuable secret. The valuable secret can be either a secret from outside the system (called PKI-assured non-transferability) [4] or all secrets and credentials inside the system (called all-or-nothing non-transferability) [5]. In [4] each user has a master public key which can be registered and its corresponding master private key can be used to sign “important legal or financial documents”. Lysyanskaya et al. state that it is impossible to share a credential without sharing the master private key. This way the user’s knowledge is made valuable beyond its primary intent and therefore it is assumed the user won’t share it. Thus, the system’s secret is personalised to the user and does not necessarily have to be kept secret from him. It is worth mentioning that issuing a credential can be done by an interactive protocol between issuer and user without revealing the user’s credential or valuable secret to the issuer. Although it may be tough for the issuer to verify the secret’s accuracy.

Biometric Access Control. As suggested by Bleumer the wallet with observer model can be extended by adding a biometric facility to the observer [6]. Before
starting the proof of knowledge the observer checks the user’s biometrics. This could be done by using a smartcard with embedded fingerprint reader [10] or so called match-on-card systems, where an external reader delivers the biometrics straightly to the card. However, the advantage of embedding the fingerprint reader into the card to match-on-card systems is, that the user’s biometrics are not put on risk like it has already occurred with PINs of cash cards by manipulated PIN-readers. We therefore assume an implementation with an embedded fingerprint reader for further consideration.

Security of the System. Before dealing with scenarios and an attacker model in the next section we need to have a look at the integral parts of the credential system’s security. These components can be divided into three groups: The security of the basis credential system (G) and the security of the efforts trying to make those credentials untransferable, either by biometric access control (B) or by embedding a valuable secret (S).

Moreover, the security of non-transferable anonymous credentials depends mostly on the following points:

(G1) The security of the underlying cryptographic functions as stated above, e.g. the used zero-knowledge-proof, blind or group signature schemes.
(G2) The secrecy of the credentials created by the issuer when initialising the smartcard or combining them with an embedded valuable secret.
(B1) The quality of the deployed device’s tamperproofness.
(B2) The difficulty of circumventing the biometric sensors.
(S1) The value of the embedded secret.
(S2) The precautions taken by the users in combination with the system’s potential to prevent loss, duplication or unauthorised use of credentials.
(S3) The strength of the connection between the anonymous credential and the embedded valuable secret.

3 Scenario and Attacker Model

Scenario. There are at least two cases where untransferable anonymous credentials are useful. The first instance tries to prevent infringements by making the user proving a certain attribute, e.g. proof of age, driving licenses, a country’s citizenship or special abilities such as academic degrees. These proofs have in common that they realise a kind of access control to enforce laws. People who are of legal age may buy alcohol and tobacco in stores, people who own a driving license may rent cars. In the second case anonymous credentials act as tickets for a given service. Either the service is paid in advance, e.g. weekly or monthly tickets for travelling by train or visiting a pool, or the ticket permits its owner a particular discount, e.g. seniors, student or handicapped ID or the German Railways BahnCard. It may not be obvious at a first glance, but the difference between the two scenarios is in the injured party if the system is circumvented. The first scenario’s aggrieved party is the issuer who wants to enforce a certain law while in the latter scenario the user can obtain a service by fraud or at least cheaper and thus the verifier is or belongs to the injured party.
**Attacker Model.** There are several parties involved in a working anonymous credential system: the issuer, the user and the verifier of the credential, and the manufacturer of the used software and hardware, and – especially when using biometric access control – the tamperproof devices. Since our main focus is a comparison of the strengths and weaknesses of both approaches in respect of the credentials’ untransferability, we make several assumptions to narrow the field of possible attacking parties. First of all, we do not address third party’s attacks since – depending on their goal – they will have less power than the involved parties. If a third party wants to gather information about the user the verifier can be considered more powerful since he already interacts with the user. If we study attacks on the credential system or the credential’s untransferability the user is more powerful since he already has a valid credential. We also assume that anonymous credentials will not be used in high-security environments. Therefore, we adopt a more practical view on the security of the system.

Furthermore, we imply that each party uses only trustworthy hard- and software for its own devices with no backdoors, Trojan horses, etc. We note that the tamperproof device used for biometric access control is a shared device. Since it is operated by the user but either the issuer (first scenario) or the verifier (latter scenario) wants to be sure it executes only trustworthy operations. Due to the fact that the user does not need to trust the tamperproof device here, because we rely on the wallet with observer architecture, it is reasonable to concede the choice of the tamperproof device to the issuer respectively the verifier.

While the verifier has a natural interest to prove the credential in the latter scenario we suppose he has at least a reasonable interest to do so in the first scenario. This assumption is based on the observation that either the verifier, e.g. a police officer, has a certain relationship to the issuer or the verifier is forced to carefully prove the credential by a third party, e.g. the state or an insurance company. Thus, a dishonest verifier’s aim is most likely to gather information about the user. In addition to transferable anonymous credentials the verifier may want to glean the user’s embedded secret or some of his biometric data. But since we assume the wallet with observer architecture does not leak any biometrics and the embedded secret provides the verifier no additional point of attack, we conclude the verifier is only capable of attacking the underlying credential system even if the embedded secret may raise his incentive to do so.

We further assume that the issuer generates credentials or initialises the tamperproof device without leaking any secret information to the user or verifier and vice versa that a protocol is used that does not reveal the user’s valuable secret [4, 5] or biometrics to the issuer.

This leaves us with one possible attacker, the user. So we need to take a closer look at his goals. If the user is seen as an attacker his aim is to trick the authentication either by creating his own credentials or by sharing a valid credential with other persons. As stated above if the credential can be transferred or the system is broken, it can be easily seen that in most cases either a law is circumvented (first scenario) or the verifier is the aggrieved party (latter scenario).
4 Attacks on Untransferability

In the previous section we narrowed the field down to one attacker: the user who wants to share or forge credentials. This section aims to compare how biometric access control and embedded valuable secrets fulfil their needs. When taking a closer look at the integral parts of the credential system’s security it is obvious that both approaches do not differ much in the security of the basis credential system (G). As we are interested in a comparison of the provided security we can disregard (G1,2). This reduces our evaluation to approach specific security (B1,2) versus (S1-3). Before going into detail we discuss a general attack on the wallet with observer architecture which can also be applied if the untransferability of the credential shall be provided by an embedded secret. The verifier cannot be sure if the user is in radio contact with a legitimate user (and smartcard) who is willing to accomplish the authentification for him. Since this affects both approaches we do not invest more effort here. When evaluating attacks on the approach using biometric access control there are two points of attack, the tamperproof device and the biometric sensor. Since the biometric sensor is embedded in the device and therefore has probably only a moderate security level, it is reasonable to neglect (B1) and consider (B2) the weakest point. Many reports on circumvention of biometric systems like the use of photos with iris codes or facial age verification or forged fingerprints suggest that unattended biometric access control, e.g. online or automated age verification, is susceptible to fraud while it may be harder, but not unfeasible, to circumvent attended verification, e.g. at a bar.

Regarding the security of embedded secrets it is evident that (S2) strongly depends on (S1). Only if the embedded secret has some value to the user, he takes care to protect it. On the other hand if the system is set up carefully it seems unfeasible to the user to detach the embedded secret from the credentials. We therefore claim that the value of the secret is most important concerning this approach. To find a reasonable valuable secret is a quite hard problem. On one hand the proposed master secret key in [4] seems capable of preventing most users from sharing, on the other hand using such a powerful key seems disproportional and dangerous to protect low value credentials. Of course, if such a powerful credential already exists for other purposes it may be used to protect many other credentials of less value. Comparing both approaches we showed that deciding which approach suits better is an estimation between the user’s ability to circumvent the biometric sensor versus the value of the embedded secret he might be ready to risk.

5 Conclusion

As the previous section shows, neither biometric access control nor embedded valuable secrets ensure the untransferability of anonymous credentials. While biometric access control is the more expensive and probably more error-prone solution, it might be hard to find valuable secrets to really prevent the sharing of credentials. The main disadvantage of biometric access control is that
unattended biometrics seems feasible to bypass and the biometric’s missing universality might restrict its usage. Otherwise biometric access control limits the possibility of unintentionally sharing the credentials for free and if the biometric measurements are attended it seems applicable. Embedded valuables in contrast raise the system’s value and thus the incentive of stealing them (with the underlying credentials) or breaking the system’s architecture. For low value credentials it may be possible to put a certain amount of the user’s money at risk if he shares his credential, but naturally this won’t prevent all users from sharing. If there already exists a valuable credential, credentials with less value can be bound to it, but even then the user might decide to share, e.g. with close family members. The following table overviews the elaborated attributes of both approaches:

<table>
<thead>
<tr>
<th>attribute</th>
<th>biometrics</th>
<th>embedded secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>circumvention depends on</td>
<td>(un)attended access control</td>
<td>secret</td>
</tr>
<tr>
<td>universality depends on</td>
<td>biometrics</td>
<td>secret</td>
</tr>
<tr>
<td>tamperproof device</td>
<td>with biometric reader</td>
<td>not needed</td>
</tr>
<tr>
<td>unintended sharing</td>
<td>unlikely</td>
<td>may occur</td>
</tr>
<tr>
<td>system’s value</td>
<td>unchanged</td>
<td>raised</td>
</tr>
</tbody>
</table>

Acknowledgement

The author is grateful to Lexi Pimenidis for helpful discussions and comments and to the anonymous reviewers for their feedback and suggestions.

References