A Survey on Non-transferable Anonymous Credentials

Sebastian Pape
pape@db.informatik.uni-kassel.de

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 paper seeks to identify possible fields of application and to compare both approaches with respect to the credentials' non-transferability.
The paper shows that both approaches do not ensure the non-transferability of anonymous credentials, but may be applicable in some fields. On the one hand, it might be hard to find valuable secrets to really prevent the sharing of credentials, in particular with close family members. On the other hand, biometric sensors embedded in a smartcard can be circumvented with some effort, especially if access control is unattended. Although the combination of both approaches may prevent more users from sharing their credentials, it suffers from restrictions of both approaches and from the effort needed to put it in place.
However, assuming that anonymous credentials will probably not be used in high-security environments, both approaches might be sufficient to prevent sharing in some applications. If the users already possess personal digital assistants, embedded valuable secrets are a quite cheap solution, even though they raise the system's value. If access control is attended, biometric sensors are reasonably safe and limit the possibility of unintentionally sharing the credentials for free.

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. Here anonymous authentication means that the verifier should not gather any information about the user except that the user is authorised. 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 credentials is undesired. People who have to prove their age to an organisation for the purchase of alcoholic drinks or tobacco or if they want to visit a bar or discotheque, are an example of this scenario. If the organisation

is not considered trustworthy by 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 without involving his relatives or friends who could prove the statement instead. Other examples for utilising anonymous credentials include the proof of a country's citizenship, driving license 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 [4–6] or even all of the user's secrets inside the system, namely credentials from other issuers [7]. Another possibility of assuring non-transferability of anonymous credentials is to make use of biometric control devices [8]. Of course, it should be guaranteed that these devices do not break the user's anonymity.
This paper seeks to elaborate on the advantages and disadvantages of both approaches with regard to the non-transferability of credentials. The next section describes anonymous credentials and possible implementations, while Sect. 3 introduces our scenario and attacker model. Section 4 investigates the approaches' non-transferability and leads to the conclusions in Sect. 5.

2 Anonymous Credentials

The basic idea of anonymous credentials is that users are able to anonymously prove attributes issued by an organisation. As stated above, anonymous authentication means that neither should the verifier learn any information about the user except that the user is authorised nor should he be able to link several authentications of the same user which would allow him to build profiles on authenticating users.
Implementations usually access proofs of knowledge in combination with blind signature [9] and group signature [10] schemes.
"Knowledge" is only one authentication factor [11, 12], but it can easily be transformed to "possession" by moving the secret into a smartcard, where we presume it cannot be copied from. More precisely we assume the user is able to use the credential without the credential leaving the card. 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 [13]. 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 the 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 personal identification number (PIN) resulting in a two-factor-authentication (possession of card and knowledge of the PIN) as already known from today's cash cards.

2.1 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*) [4–6] or all secrets and credentials inside the system (called *all-or-nothing non-transferability*) [7]. In [6] each user has a master public key and should be strongly encouraged to keep the corresponding master private key secret. This can be realised for example by registering the public master key at a certification authority as a legal digital signature key which 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 will not share it. Thus, the system's secret is personalised for each user and does not necessarily have to be kept secret from him. This offers two possible implementations: the above concept of embedding the key into a smartcard or delivering a personalised secret to the user. The latter is possible because the user is not technically prevented from sharing his credential. Instead, as aforementioned, it is assumed he does not want to share the additional embedded valuable secret. It is worth mentioning that issuing a credential can be realised by an interactive protocol between issuer and user without revealing the user's credential or valuable secret to the issuer. However, it may be tough for the issuer to verify the secret's accuracy.

2.2 Biometric Access Control

As suggested by Bleumer, the wallet with observer model can be extended by adding a biometric facility to the observer [8, 14]. Before starting the proof of knowledge the observer checks the user's biometrics. This could be implemented using a smartcard with embedded fingerprint reader [15] or so called *match-on-card* systems [16] where an external reader delivers the biometrics directly to the card. The advantage of embedding the fingerprint reader into the card to match-on-card systems is that the user's biometrics are not put at risk as has already occurred with PINs of cash cards by manipulated PIN-readers [17]. Contrary to the user's PIN, one may not consider his fingerprints secret, because they cannot be changed and he leaves them anywhere, e.g. at the shop's door. But even if the dealer could get the user's fingerprint at his shop's door, this would require a much larger effort than an automatic acquisition of the user's biometric. Thus, the user's privacy would be invaded by an automatic acquisition of his fingerprints. We therefore assume an implementation with an embedded fingerprint reader in the following.

2.3 Other Approaches

Besides the two well-investigated approaches discussed above one may think of other schemes to prevent users from sharing their credentials. We first need to point out that the biometric access control described in the previous subsection is actually operating against the user. He is not allowed to have his credentials available as pleased to prevent him from passing them around. Thus, it is quite obvious that "traditional access control schemes" such as passwords may not be useful in this case. The most obvious idea for a new approach is to use a combination of the two approaches discussed above. We will take this into account when investigating the approaches' non-transferability in section 4.
In the last years some scientists and technophiles had radio-frequency identification (RFID) chips implanted [18, 19]. On the one hand, if the user really trusts all parties involved in the production and implantation of the RFID chip, namely manufacturer and surgeon, this may be an option. On the other hand, the user risks an intrusion into his privacy here. Since the user cannot be sure about the chip's transmission, even if there are some means of control over chip's transmission, the verifier may be able to communicate directly with the chip. Thus, the wallet with observer architecture does not apply here and the user has to trust other parties with all the consequences regarding his privacy. Furthermore, the system's setup seems to be quite complicated and the connection between the user and the chip can simply be broken by another surgeon. Thus, we argue that implanted RFID chips are inappropriate and do not consider them any further in this paper.

2.4 Integral Parts of the Credential System's Security

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 non-transferable, 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.

2.5 Limiting the Consequences of Abuse

To limit the effect of dishonest users the issuer may want to limit the number of available tokens per time period. Damgård et al. proposed a scheme to allow only one anonymous authentication at a time [20]. Later, Camenisch et al. improved this approach by creating a credential system that lets a user anonymously authenticate at most n times per given time period [21]. The basic idea is that each user has a dispenser which automatically refreshes and creates n tokens every time period. Each token can only be used once and should a token be used twice the verifier is able to revoke the user's anonymity. Camenisch et al. also offer *glitch protection* for basically honest users who only occasionally reuse their tokens for instance if the user's operation system crashes. In this case, he may not know which tokens have already been used and thus mistakenly uses a token twice, even though unused tokens would have been available to him.
Of course the scheme itself does not provide non-transferability of credentials in any way, but in combination with the precautions stated earlier in this section it limits the extent of abuse if the number of available tokens per time period is chosen appropriately.

3 Scenario and Attacker Model

3.1 Scenario

There are at least two cases in which non-transferable anonymous credentials are useful. The first instance tries to prevent infringements by making the user prove 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 lies 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 cheaper or by fraud and, thus, the verifier is, or belongs to, the injured party.

3.2 Attacker Model

There are several parties involved in an anonymous credential system: the issuer, the user and the verifier of the credential. Furthermore, the manufacturer of the software and hardware needs to be trustworthy, especially when using biometric access control and, therefore, tamper-proof devices are needed. Since our main focus lies on the comparison of the strengths and weaknesses of both approaches

with respect to the credentials' non-transferability, 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 non-transferability 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 and that the attacking costs are proportionate to the assessed breach win. 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 tamper-proof device used for biometric access control is a shared device, since it is operated by the user and 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 tamper-proof device here because we rely on the wallet with observer architecture, it is reasonable to concede the choice of the tamper-proof device to the issuer or the verifier, respectively.
While the verifier has a natural interest to prove the credential in the latter scenario we suppose he shows at least 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, the aim of a dishonest verifier is most likely to gather information about the user and to break his privacy. In addition to transferable anonymous credentials the verifier may want to investigate 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 provide him a stronger incentive to do so.
We further assume that the issuer generates credentials or initialises the tamper-proof 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 [6, 7] or biometrics to the issuer.
This leaves us with one possible attacker, the user, and 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 aggrieved (latter scenario).

4 Attacks on Untransferability

4.1 General Attacks

Before going into detail about the attacks on the specific approaches we discuss a general attack on the wallet with observer architecture which can also be applied if the non-transferability of the credential is 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 authentication for him (see Figure 1). A simple but hard to implement countermeasure would be to isolate the user during authentication to prevent him from communicating with others. Another approach, distance-bounding protocols, measures round-trip-times to prevent relay attacks and was proposed by Beth and Desmedt [22] and the first concrete protocol was introduced by Brands and Chaum [23]. Drimer and Murdoch describe an implementation of this defence for smartcards which requires only modest alterations to current hardware and software [24]. Even though the setup is slightly different from [24], since the smartcard in the wallet with observer architecture is not allowed to communicate directly with the verifier to protect the user's privacy, distance-bounding protocols provide an opportunity to prevent or limit relay attacks, if appropriate timing constraints are chosen. Since this attack affects both approaches we do not further elaborate on relay attacks and their countermeasures in this paper.

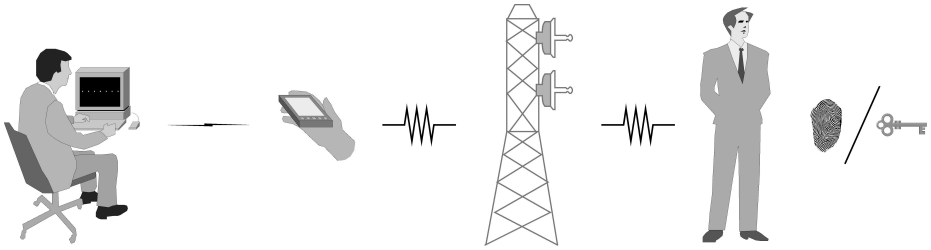

Fig. 1. If they are able to communicate, a bogus and a legitimate user could share a credential.

4.2 Attacks on the Specific Approaches

In the previous section we narrowed down the field 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 (see section 2.4) it is obvious that both approaches do not differ much as far as the security of the basis credential system (G) is concerned. As we are interested in comparing

the provided security we can disregard (G1,2). This reduces our evaluation to approach specific security (B1,2) versus (S1-3).

Biometric Access Control. When evaluating attacks on the approach using biometric access control there are two points of attack, the tamper-proof device and the biometric sensor. Since the biometric sensor is embedded in the device and, therefore, only has probably a moderate security level, it is reasonable to neglect (B1) and consider (B2) the weakest point. Many reports on circumvention of biometric systems include the use of photos with iris codes or facial age verification or forged fingerprints and 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.
This suggests that biometric access control restricts the group of people who are able to share a credential to those who are experts in biometric sensors or tamper-proof devices or at least profit from the experts' work.

Embedded Valuable Secrets. 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 for this approach. To find a reasonably valuable secret is quite a problem. On the one hand, the proposed master secret key in [6] 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. However, if such a powerful credential already exists for other purposes it may be used to protect many other credentials of smaller value.
We also note that these valuables might not prevent all users from sharing; be it they share their credentials incautiously, be it they really trust someone else, e.g. a close family member. Having this in mind, we refer only to users intentionally sharing credentials, e.g. parents sending their children to buy them alcohol or tobacco from a store.
A minor drawback for this approach is the possibility of a revocation of the master key, which would make the embedded secret useless. Since it is assumed that the embedded key is very powerful, and thus valuable, it is inevitable to let the user revoke it. This allows the user to immediately end the validity of a previously shared credential for the cost of needing a reinitialisation of his credentials (the master key and all keys depended on it). Obviously a simple countermeasure is to make the user pay for each reinitialisation as it is already common for example with cash cards or SIM cards. The price of the reinitialisation and the possible savings determine if this is a profitable deal for the user.
Another advantage considering anonymous credentials with embedded values is that they do not necessarily need an extra device. For example, concerning age verification at an online shop, it would be enough to have additional software

on the already available computer. But in this case the credential is most likely in a very dangerous environment and can easily be stolen if the computer is compromised. A way to prevent this would be to delegate this task to a smart card. Which of those approaches is the most suitable is mainly a trade-off between the quality of the embedded valuable secret, the required strength of non-transferability, and the economic costs.

Combining Embedded Valuable Secrets and Biometric Access Control. Comparing both approaches we have shown that the decision which approach is most suitable 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. A combination of both approaches seems to be promising regarding the non-transferability, since a possible attacker has to circumvent the biometric sensors or break the tamper-proof device and, furthermore, the owner of the credentials must be willing to share his secret. Otherwise not only the benefits accumulate but also the restrictions. Users must have usable fingerprints and a valuable secret which they are willing to embed into the system. The combination of the approaches is the most expensive, since each user needs a tamper-proof device with embedded fingerprint reader and the system has to be linked to an already existing "legal digital signature certification authority" which probably will not be free of charge.

5 Conclusion

As the previous section shows, neither biometric access control nor embedded valuable secrets ensure the non-transferability 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, especially since the user is able to revoke the sharing at any time. Table 1 gives an overview on the elaborated attributes of both approaches.
The main disadvantage of biometric access control is that it seems feasible to bypass unattended biometric access controls and that 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. Furthermore, by the use of tamper-proof devices the cloning of credentials gets quite hard and, thus, the issuer can be at least reasonably sure the credential is not cloned.
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 will not prevent all users from sharing. If there already exists a valuable credential, credentials of lower value can be bound to it, but even then the user might decide to share, e.g. with close family members. To avoid unintentional sharing of the credential the user must be very careful or has to additionally use a tamper-proof

device to protect his credentials.
Also, the combination of both approaches is not the answer to all drawbacks. While it may prevent more users from sharing it suffers from restrictions of both approaches and from the effort needed to put it in place. Nevertheless, it is important to keep in mind that all approaches are not able to assure non-transferability if the user cannot be isolated but is able to communicate with the outside world during authentication. Therefore, all implementations need to take defences against relay attacks into account, e.g. based on distance-bounding protocols.

Table 1. Attributes of different approaches to ensure non-transferability: biometric access control, embedded valuable secret, a combination of both approaches, and embedded valuable secret with a tamper-proof device.

attribute	biometrics	embedded secret
circumvention depends on	(un)attended access control	secret
circumvention by	experts	close family members
tamper-proof device	with biometric reader needed	not needed
universality depends on	biometrics	secret
credential cloning	hard	easy
unintended sharing	unlikely	may occur
system's value	unchanged	raised

attribute	biometrics & embedded secret	embedded secret (TP)
circumvention depends on	(un)attended AC & secret	secret
circumvention by	trusted experts	close family members
tamper-proof device	with biometric reader needed	needed
universality depends on	biometrics & secret	secret
credential cloning	hard	medium
unintended sharing	unlikely	unlikely
system's value	raised	raised

Acknowledgement

The author is grateful to Lexi Pimenidis for helpful discussions and comments on an earlier version of this work and to the anonymous reviewers for their feedback and suggestions. The author also thanks the participants of the Summer School for their annotations and fruitful discussions.

References

1. D. Chaum: Security without identification: transaction systems to make big brother obsolete. Communications of the ACM, vol. 28, pages 1030 – 1044, 1985.

2. D. Chaum, J.-H. Evertse: A secure and privacy-protecting protocol for transmitting personal information between organizations. Advances in Cryptology – CRYPTO '86, pages 118 – 167, Springer, 1987.
3. D. Chaum: Blind Signatures for Untraceable Payments. Advances in Cryptology – CRYPTO '82, pages 199 – 203, Springer, 1983.
4. C. Dwork, J. Lotspiech, M. Naor: Digital Signets: Self-Enforcing Protection of Digital Information. Proceedings on Theory of Computing, 28th Ann. ACM Symp., 1997.
5. O. Goldreich, B. Pfitzmann, R. L. Rivest: Self-Delegation with Controlled Propagation — or — What If You Lose Your Laptop. Proceedings on Advances in Cryptology - CRYPTO '98, Lecture Notes in Computer Science, vol. 1462, pages 153 – 168, Springer, 1998.
6. A. Lysyanskaya, R. L. Rivest, A. Sahai, S. Wolf: Pseudonym Systems. Proceedings on Selected Areas in Cryptography, 6th Annual International Workshop, SAC '99, LNCS, vol. 1758, pages 184 – 199, Springer, 2000.
7. J. Camenisch, A. Lysyanskaya: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. Advances in Cryptology – EUROCRYPT 2001, LNCS, vol. 2045, pages 93 – 118, Springer, 2001.
8. G. Bleumer: Biometric yet Privacy Protecting Person Authentication. LNCS, vol. 1525, pages 99 – 110, 1998.
9. D. Chaum: Blind signatures for untraceable payments. Advances in Cryptology – Crypto '82, Springer-Verlag, pages 199 – 203, 1983.
10. D. Chaum and E. van Heyst: Group signatures. Advances in Cryptology – EUROCRYPT '91, LNCS, vol. 547, pages 257 – 265, 1991.
11. FFIEC Press Release: Authentication in an Internet Banking Environment. Techreport, Federal Financial Institutions Examination Council, 2005.
12. J. Brainard, A. Juels, R. Rivest, M. Szydlo, M. Yung: Fourth Factor Authentication: Somebody You Know. CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, ACM, pages 168 – 178, 2006.
13. D. Chaum, T. P. Pedersen: Wallet Databases with Observers. Advances in Cryptology – CRYPTO '92, LNCS, vol. 740, pages 89 – 105, Springer, 1993.
14. R. Impagliazzo, S. M. More: Anonymous Credentials with Biometrically-Enforced Non-Transferability. Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society (WPES '03), pages 60 – 71, 2003.
15. Homepage of Biometric Associates, Inc.: http://www.biometricassociates.com.
16. S. B. Pan, Y. H. Gil, D. Moon, Y. Chung, C. H. Park: A Memory-Efficient Fingerprint Verification Algorithm Using a Multi-Resolution Accumulator Array. ETRI Journal, vol. 25,pages 179 – 186, 2003.
17. M. Barwise, D. Bachfeld: Attack of the card cloners. IT security news and services at heise Security UK, http://www.heise-online.co.uk/security/features/print/100187, 2007.
18. K. Finkenzeller: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley and Sons, 446 pages, 2003.
19. A. Graafstra: RFID Toys: 11 Cool Projects for Home, Office and Entertainment. Wiley, 336 pages, 2006.
20. I. Damgård, K. Dupont, M. O. Pedersen: Unclonable Group Identification. EUROCRYPT 2006: 555-572 Advances in Cryptology – EUROCRYPT 2006, LNCS, vol. 4004, pages 555 – 572, 2006.
21. J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, M. Meyerovich: How to win the clonewars: efficient periodic n-times anonymous authentication.

CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, ACM, pages 201 – 210, 2006.
22. T. Beth, Y. Desmedt: Identification tokens – or: Solving the chess grandmaster problem. Advances in Cryptology – CRYPTO '90, LNCS, vol. 537, pages 169 – 177, Springer, 1991.
23. S. Brands, D. Chaum: Distance-bounding protocols. Advances in Cryptology – EUROCRYPT '93, LNCS, vol. 765, pages 344 – 359, Springer, 1994.
24. S. Drimer, S. J. Murdoch: Keep your enemies close: distance bounding against smartcard relay attacks. SS'07: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, USENIX Association, pages 1 – 16, 2007.