Practical Revocable Anonymous Credentials

Jan Hajny * and Lukas Malina

Brno University of Technology,
Department of Telecommunications, Brno, Czech Republic
{jan.hajny,lukas.malina}@phd.feec.vutbr.cz

Abstract. Currently, there are many solutions for authentication. Mostly, the authentication protocols based on traditional cryptographic constructions, such as digital signatures, hash functions and symmetric encryption schemes, are used. To provide more privacy protection, credential systems were introduced. Using these systems, users can anonymously prove that they possess some attributes. The attributes can represent anything from the age of users to their citizenship or, e.g., driving license possession. The main problem of these systems is revocation since it is currently impossible to efficiently revoke invalid users, attackers or users who use stolen identities. In this paper, a novel conception for anonymous credentials with practical revocation is proposed.

Keywords: Privacy, Revocation, Credential Systems, Anonymity

1 Scheme Description

In this paper, we present a new concept for credential systems. The concept supports all privacy-enhancing features individually provided by related solutions, namely *anonymity, unlinkability, untraceability, non-transferability* and *attribute proofs*. Additionally, our novel concept allows efficient and practical off-line revocation. There are 4 entities in our credential scheme. They are the Issuer (I) who issues attributes, the Verifier (V) who verifies attributes, the User and the Public Authority (PA) who allows revocation. Each attribute (like citizenship, age or driving license possession) is assigned a unique public value A_j. The list of these links between A_j's and their meaning is published and maintained by PA. All Users in the system who want to be issued j^{th} attribute can download its value A_j from this public list. All Users share the same values thus it is not possible to distinguish particular Users by the attribute value A_j. To exclude unauthorized users, each valid user is given private keys for each attribute in the Issuance phase.

Credential Issuance Phase
To use A_j for verification, proper keys must be provided to the User by PA and Issuer. Thus, each valid user is provided an attribute A_j together with keys

* Jan Hajny was supported by the Fulbright stipend.

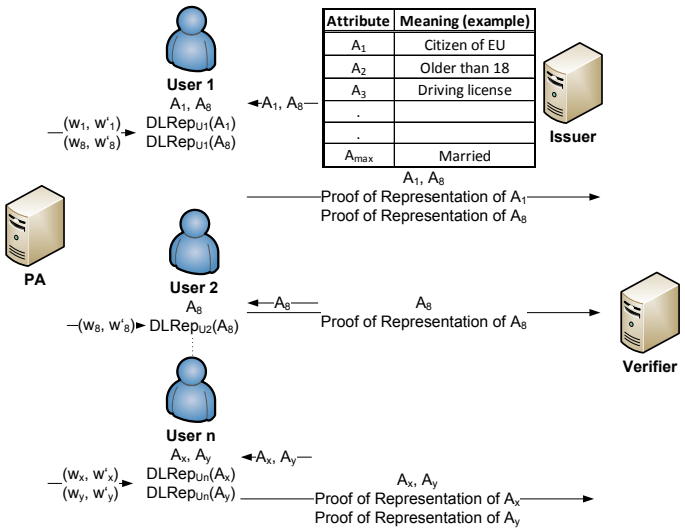

Fig. 1. Proposed Principle

(w_j, w'_j) by I and PA before he can give proofs about the attribute ownership. The attribute value A_j is the same for all Users but keys (w_j, w'_j) are unique for each User. The keys are the discrete logarithm representation of A with respect to generators g_1, g_2 in modulo n such that $A_j = g_1^{w_j} g_2^{w'_j} \bmod n$. In our proposal, we use Okamoto-Uchiyama (OU) group [3] defined by generators g_1, g_2 and modulus $n = r^2 s$ where r, s are large primes. There is a huge number of possible representations of A_j so it is possible to provide all Users with unique keys. By employing an advanced cryptographic protocol for issuance, keys are provided to Users only, no other entity learns them.

Credential Verification Phase

Having the proper keys, a User can run the credential verification protocol which is a proof of knowledge of discrete logarithm of A_j with respect to g_1, g_2. The protocol can be denoted as $PK\{(w_j, w'_j) : A_j = g_1^{w_j} g_2^{w'_j}\}$. Users unaware of proper keys are always rejected by the protocol because they don't know the representation. Valid users are stuck to their keys because of the binding property of A_j (it is infeasible to compute different representation of A_j without factoring n). This protocol is completely zero-knowledge so no extra information leaks except that the User has proper keys (w_j, w'_j). Each session is randomized by a random number r which stays secret but is present in the form of a verifiable encryption (VE) in the protocol. The randomization makes all sessions completely unlinkable thus verifiers cannot create user profiles. Since all users share the same A_j, it is impossible to trace the User, identify the User or profile the User.

Credential Revocation Phase
In some cases, it is necessary to revoke Users. For this reason, an entity called Public Authority is introduced. The Public Authority knows a trapdoor to Okamoto-Uchiyama group, thus can decrypt randomness r used in the verification protocol. Using the randomness, PA can reconstruct unique keys (w_j, w'_j). These keys can be later used to identify malicious users and attackers, but only in cooperation with Issuers. By such a distribution, we protect Users against privacy disclosure done by a single entity. The approach is based on the assumption that it is unlikely that more entities (both Issuer and PA) would cooperate in unlawful breaking of Users' privacy.
The full system specification is still in progress and the cryptographic details will be provided in the full paper. In the meanwhile, we enlist the constructions used: Okamoto-Uchiyama trapdoor one-way function [3], Σ-protocols [2], Bao's verifiable encryption [1] and discrete logarithm commitments. The scheme conception is depicted in Figure 1[1].

Conclusion

Using the proposed system, users can anonymously provide proofs about their age, citizenship or other attributes. This functionality significantly improves privacy since users are not required to unnecessary disclose their identity and private data any more. Unlike existing systems, our system provides efficient revocation. The conception proposed in this paper is currently being implemented on smart-cards. The first implementation results show that the scheme is highly practical, with the time of verification under 1 s using an off-the-shelf smart-card.

Acknowledgment

Jan Hajny is the Holder of Brno Ph.D. Talent Financial Aid - Sponsored by Brno City Municipality. Research was sponsored by the Technology Agency of the Czech Republic and the MSMT grant FRVS 823/2012/F1.

References

1. Bao, F.: An efficient verifiable encryption scheme for encryption of discrete logarithms. In: Schneier, B., Quisquater, J.J. (eds.) Smart Card. Research and Applications, Lecture Notes in Computer Science, vol. 1820, pp. 213–220. Springer Berlin / Heidelberg (2000)
2. Cramer, R.: Modular Design of Secure, yet Practical Cryptographic Protocols. Ph.D. thesis, University of Amsterdam (1996)
3. Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: Nyberg, K. (ed.) Advances in Cryptology - EUROCRYPT 98, Lecture Notes in Computer Science, vol. 1403, pp. 308–318. Springer Berlin / Heidelberg (1998)

[1] Please be advised that (w_8, w'_8) of User 1 is different from (w_8, w'_8) of User 2. Although not distinguished by notation, User keys are always different, even for same attributes.