Digital credential

From Wikipedia, the free encyclopedia
Jump to: navigation, search
Ambox scales.svg

This article has been nominated to be checked for its neutrality. Discussion of this nomination can be found on the talk page. (December 2007)

This article is written like a personal reflection or essay and may require cleanup. Please help improve it by rewriting it in an encyclopedic style. (March 2008)

Digital credentials are meant to be the digital equivalent of paper based credentials. Just as an example a paper based credential could be a passport, a Driver's license, a membership certificate or some kind of ticket to obtain some service, like a cinema ticket or a public transport ticket. A credential is a proof of qualification, competence, or clearance that is attached to a person. Similarly digital credentials prove something about their owner. Both may contain personal information such as the persons name, birthplace, and birthdate, or biometric information such as a picture or a finger print.

Because of the still evolving and sometimes conflicting terminologies used in the fields of computer science, computer security, and cryptography, the term credential is used quite confusingly in these fields. Sometimes passwords or other means of authentication are referred to as credentials. In operation system design credentials are the properties of a process (such as its effective UID) that are used for determining its access rights. On other occasions certificates and associated key material such as those stored in PKCS#12 and PKCS#15 are referred to as credentials.

Often however digital credentials, like digital cash, are only associated with anonymous digital credentials. Such credentials, while still making an assertion about some property, status, or right of their owner, do not reveal the owner's identity.

Contents
[hide]

[edit] Real world, digital world analogy

Real world credentials are a diverse social phenomenon, and as such are difficult to define. As with digital signatures it is misleading to assume a direct correspondence between the real-world and the digital concept. This holds even if defining criteria for credentials in the digital world could be agreed on.

Let us look at the lot of digital signatures. On the one hand the success of digital signatures as a replacement for paper based signatures has lagged behind expectations. On the other hand many unexpected uses of digital signatures were discovered by recent cryptographic research. A related insight that can be learned from digital signatures is that the cryptographic mechanism need not be confused with overall process that turns a digital signature into something that has more or less the same properties as a paper based signature. Electronic signatures such as paper signatures send by fax may have legal meaning, while secure cryptographic signatures may serve completely different purposes. We need to distinguish the algorithm from the process.

[edit] Digital cash and digital credentials

Why is it that digital cash is associated with digital credentials, while paper or metal coins are usually not considered to be genuine real world credentials? Money is usually not seen as a qualification that is attached to a specific person. Token money is taken to have a value on its own. We now consider a specific property of digital assets. They are easily copied. Consequently digital cash protocols have to make an extra effort to avoid the double spending of coins. Remember that credentials are a proof of qualification that is attached to a person. Digital cash uses the following technique. E-Coins are given to individuals, who cannot pass them on to others, but can only spend them with merchants. As long as they spend a coin only once, they are anonymous, but should they spend a coin twice, they become identifiable and appropriate actions can be taken by the bank. This commonality, the binding to an individual, is why digital cash and digital credentials share many commonalities. In fact most implementations of anonymous digital credential also realise digital cash.

[edit] Anonymous digital credentials

The main idea behind anonymous digital credentials is that users are given cryptographic tokens which allow them to prove statements about themselves and their relationships with public and private organizations anonymously. This is seen as a more privacy friendly alternative to keeping and using large centralized and linkable user records.[1] Anonymous digital credentials are thus related to privacy and anonymity. Paper world analogues of such credentials are passports, driving licenses, and money. Further examples include credit cards, health insurance cards, cinema and public transport tickets, club membership cards, and game-arcade tokens. Credentials are issued by organizations that ascertain the authenticity of the information and can be provided to verifying entities on demand.

In order to investigate certain privacy specific properties of credentials, we take a more detailed look at two kind of 'credentials', physical money and credit cards. Without doubt both of them provide adequate information for doing payment transactions. However the amount and quality of the information disclosed varies. Money is protected from forgery by its physical properties. Beyond that, only very little information is revealed: Coins feature an engrained value and the year of coining; in addition bank notes contain a unique serial number in order to provide the traceability required by law enforcement.

On the other hand the use of a credit card, whose main purpose is similar to money, allows for the creation of highly detailed records about the card owner. The main privacy advantage of money is that its users can remain anonymous. There are however other security and usability properties that make real world cash popular.

Credentials used in a national identification system are also especially privacy relevant. Such an ID, be it a passport, a driver's license, or some other type of card usually contains essential personal information. In certain situations it may be advantageous to reveal only parts of the information contained on the ID, e.g., some lower limit for the person's age or the fact that the person is capable of driving a car.

[edit] Anonymous digital credentials and pseudonyms

The original anonymous credential system proposed by David Chaum[2] is sometimes also referred to as a pseudonym system.[3] This stems from the fact that the credentials of such a system are obtained from and shown to organizations using different pseudonyms which cannot be linked.

The introduction of pseudonyms[2] is a useful extension to anonymity. Pseudonyms allow users to choose a different name with each organization. While pseudonyms allow organizations to associate users with accounts, organizations cannot determine the real identities of their customers. Nevertheless using an anonymous credential certain statements about the relationship of a user with one organization, under a pseudonym, can be proven to another organization that knows the user only under a different pseudonym.

[edit] History of anonymous digital credentials

As already mentioned anonymous credential systems are related to the concept of untraceable or anonymous payments.[4] In this important work, Chaum presents a new cryptographic primitive, blind signature protocols. In such a scheme the signer neither learns the message he signs, nor the signature the recipient obtains for his message. Blind signatures are an important building block of many privacy-sensitive applications, such as anonymous payments, voting, and credentials. The original idea for an anonymous credential system[2] was derived from blind signatures, but relied on a trusted party for credential transfer—the translation from one pseudonym to another. The blind signature scheme introduced by Chaum was based on RSA signatures. Blind signature schemes based on the discrete logarithm problem can also be used for constructiong anonymous credential systems.

Stefan Brands generalized digital credentials to a great extent, with his secret-key certificate based credentials, improving on Chaum's basic blind-signature based system in both the discrete log and strong RSA assumption settings. Brands credentials provide the fullest feature set, the most efficient algorithms by a large margin, and provide privacy in an unconditional security setting. Brands has tight proofs of security, compact credential representation and messages. Brands credentials have seen commercial use in digicash, ecafe esprit project, zero-knowledge systems and credentica.[5] Brands protocls have seen wider security peer-review than the competing systems. Brands credentials are 1 to 2 orders of magnitude more computationally efficient than the comparable alternatives. They also include an efficient observer setting (augmenting security with a low performance smart card without compromising privacy guarantees). And many other features missing in competing less efficient systems such as ability to demonstrate boolean formula in the attributes, demonstrate ranges in attributes without revealing specific values, ability to combine attributes from different credentials and even different issuers, a privacy preserving black-list method using an efficient zero-knowledge proof of non-membership in the blacklist.[6]

It is worth mentioning another credential form that adds a new feature to anonymous credentials: multi-show unlinkability. These are the group signature related credentials of Camenisch et al. The introduction of Group signatures opened up the possibility of multi-show unlinkable showing protocols. While blind signatures are highly relevant for electronic cash and one-show credentials, a new cryptographic primitive, called group signature, opened new possibilities for the construction of privacy enhancing protocols.[7] As is observed in their article, group signatures bear a resemblance to Chaum's concept of credential systems.[2]

Using a group signature scheme, the members of a group can sign a message with their respective secret keys. The resulting signature can be verified by everyone who knows the common public key, but the signature does not reveal any information about the signer except that she is a member of the group. Usually there exists another entity called the group manager, who can reveal the exact identity of the signer, and handles the adding of users to and the removal of users from the group—usually by issuing or revoking group membership certificates. The anonymity, unlinkability, and anonymity revocation provided by group signatures lends itself for a variety of privacy sensitive applications like voting, bidding, anonymous payment, and anonymous credentials

An efficient constructions for group signatures was given by Ateniese, Camenisch, Joye, and Tsudik.[8] The most efficient multi-show unlinkable anonymous credential systems[9]—the latter is essentially a low profile version of idemix[10]—are based on similar ideas.[11] This is particularly true for credential systems that provide efficient means for implementing anonymous multi-show credentials with credential revocation.[12]

Both schemes are based on techniques for doing proofs of knowledge.[13][14] Proofs of knowledge relying on the discrete logarithm problem for groups of known order and on the special RSA problem for groups of hidden order form the basis for most of today's group signature and anonymous credential systems.[6][8][9][15] Moreover direct anonymous attestation a protocol for authenticating trusted platform modules is based on the same techniques.

Direct anonymous attestation can be seen as the first commercial application of multi show anonymous digital credentials, even though in this case credentials are not attached to persons, but to chips and consequently computer platforms.

From an applications' point of view, the main advantage of Camenisch et al.'s multi-show unlinkable credentials over the more efficient Brands credentials is the multi-show unlinkable property. However, this property is mainly of practical interest in an off-line setting. Brands credentials provide a mechanism that gives analogous functionality without sacrificing performance: an efficient batch issuing protocol which can simultaneously issue many unlinkable credentials. This mechanism can be combined with a privacy preserving certificate refresh process (which gives a fresh unlinkable credential with the same attributes as a previous spent credential).

[edit] References

1. ^ "PRIME Whitepaper: privacy enhanced identity management" (PDF). PRIME. 27 June 2007. https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V2.pdf.
2. ^ a b c d Chaum, David (October 1985). "Security without identification: transaction systems to make big brother obsolete". Communications of the ACM 28 (10): 1030–1044. doi:10.1145/4372.4373.
3. ^ Lysyanskaya, Anna; Rivest, Ronald L.; Sahai, Amit; Wolf, Stefan (2000). "Pseudonym systems". in Heys, Howard M.; Adams, Carlisle M. Selected Areas in Cryptography. Lecture Notes in Computer Science. 1758. Springer. pp. 184–199. doi:10.1007/3-540-46513-8_14. ISBN 978-3-540-67185-5.
4. ^ Chaum, David (1983). "Blind signatures for untraceable payments". in Chaum, David; Rivest, Ronald L.; Sherman, Alan T. Advances in Cryptology. CRYPTO '82. 0. Plenum Press. pp. 199–203.
5. ^ "Credentica". http://www.credentica.com.
6. ^ a b Brands, Stefan A. (2000). Rethinking public key infrastructures and digital certificates. MIT Press. ISBN 978-0262024914.
7. ^ Chaum, David; van Heyst, Eugene (1991). "Group signatures". in Davies, Donald W. Advances in Cryptology – EUROCRYPT '91. Lecture Notes in Computer Science. 547. Springer. pp. 257–265. doi:10.1007/3-540-46416-6_22. ISBN 978-3-540-54620-7.
8. ^ a b Ateniese, Giuseppe; Camenisch, Jan; Joye, Marc; Tsudik, Gene (2000). "A practical and provably secure coalition-resistant group signature scheme". in Bellare, Mihir. Advances in Cryptology — CRYPTO 2000. Lecture Notes in Computer Science. 1880. Springer. pp. 255–270. doi:10.1007/3-540-44598-6_16. ISBN 978-3-540-67907-3.
9. ^ a b Camenisch, Jan; Lysyanskaya, Anna (2001). "An efficient system for non-transferable anonymous credentials with optional anonymity revocation". in Pfitzmann, Birgit. Advances in

Cryptology — EUROCRYPT 2001. Lecture Notes in Computer Science. 2045. Springer. pp. 93–118. doi:10.1007/3-540-44987-6_7. ISBN 978-3-540-42070-5.

10. ^ "idemix- pseudonymity for e-transactions". IBM. http://www.zurich.ibm.com/security/idemix/.
11. ^ Camenisch, Jan; Lysyanskaya, Anna (2003). "A Signature Scheme with Efficient Protocols". in Cimato, Stelvio; Galdi, Clemente; Persiano, Giuseppe. Security in Communication Networks. Lecture Notes in Computer Science. 2576. Springer. pp. 268–289. doi:10.1007/3-540-36413-7_20. ISBN 978-3-540-00420-2.
12. ^ Camenisch, Jan; Lysyanskaya, Anna (2002). "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials". in Yung, Moti. Advances in Cryptology — CRYPTO 2002. Lecture Notes in Computer Science. 2442. Springer. pp. 101–120. doi:10.1007/3-540-45708-9_5. ISBN 978-3-540-44050-5.
13. ^ Bellare, Mihir; Goldreich, Oded (1993). "On Defining Proofs of Knowledge". in Brickell, Ernest F. Advances in Cryptology — CRYPTO '92. Lecture Notes in Computer Science. 740. Springer. pp. 390–420. doi:10.1007/3-540-48071-4_28. ISBN 978-3-540-57340-1.
14. ^ Schnorr, Claus-Peter (January 1991). "Efficient signature generation by smart cards". Journal of Cryptology 4 (3): 161–174. doi:10.1007/BF00196725.
15. ^ Camenisch, Jan; Michels, Markus (1998). "A Group Signature Scheme with Improved Efficiency". Lecture Notes in Computer Science. 1514. Springer. pp. 160–174. doi:10.1007/3-540-49649-1_14. ISBN 978-3-540-65109-3.

[edit] See also