Anonymous Credentials: Opportunities and Challenges

Jan Camenisch

IBM Research, Zurich Research Lab
Säumerstrasse 4, CH-8803 Rüschlikon, Switzerland
jca@zurich.ibm.com

In an anonymous (or private) credential system as put forth by Chaum in 1985, a user is known to different organizations by pseudonyms only. The system allows the user to obtain a credential from one organization and then later show such credentials to another organizations without that transactions are linkable.

The area of privacy enhancing cryptography protocols and, in particular, anonymous credential systems have recently gained considerable momentum in research and indeed many substantial contributions have been made in last few years. At the same time, the interest in applying such systems in the real world has grown. Despite of this, the area is still relatively young and there are still many open research challenges to overcome.

In this talk, we will review the state of the art in anonymous credential systems. We will then discuss their applications including privacy enhancing identity management (www.prime-project.eu.org) and anonymous attestation. Finally, we will discuss research directions and challenges.

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].