Dr. Stefan Brands

740 Notre Dame Street West, Suite 1500

Montreal, Quebec

Canada H3C 3X6

Phone: +1 (514) 583.2726

Fax: +1 (514) 866.6800

E-mail: brands@cs.mgcill.ca, brands@credentica.com

Authentication

Authentication, in its most general form, is a process for gaining confidence that something is, in fact, what it appears to be. In everyday life, people continually authenticate people, objects, and other entities around them, by either consciously or subconsciously assessing *clues* that provide evidence of authenticity.

In communication and transaction settings, authentication is typically understood as the process of confirming a claimed *identity*. This involves two steps: first a *user* must present a *user identifier* (such as “John Doe” or “Employee 13579”) that uniquely represents the user in the verifier's context. The second step, *identity authentication*, involves verifying that the presenter of the user identifier is authorized to do so – in other words that the presenter is the user to whom the user identifier has been assigned.

Single-factor identity authentication ascertains that the presenter possesses something associated with the presented user identifier that is not generally accessible. This can be something the user *knows* (such as a password or a cryptographic key), something the user *has* (such as a chip card), or something the user *is* (i.e., a user biometric). Each of these three single-factor authentication methods has limitations: what the user knows may be guessed, forgotten, or shared with others; what the user has may be costly, faulty, lost, stolen, or replicated; and what the user is cannot be revoked, does not permit privacy, and requires human involvement. To strengthen the process of identity authentication, several single-factor methods may be combined, resulting in *multi-factor* authentication.

When authenticating claimed identities, verifiers implicitly place trust in the authenticity of the clues themselves. In cases where verifiers are effectively agents or proxies of the user, users can be trusted with creating their own identifiers and using their own authentication method. For example, a *self-generated* username and password suffice to protect access to one's own computer. In many communication and transaction systems, however, the security interests of verifiers and users are not aligned. In these cases, verifiers require clues that originate from *trusted parties*, also referred to as *issuers*, in order to gain confidence in the authenticity of presented user identifiers. Kerberos tickets and X.509 identity certificates are well-known examples of *certified user* *identifiers* that are issued by trusted parties; these certified identifiers contain cryptographic *authenticity marks* that are hard to forge.

When the same certified user identifiers are relied on by multiple verifiers, both users and verifiers must place tremendous trust in the issuer, which houses the power to trace, profile, and impersonate any user. For example, all user interactions with verifiers can be inescapably traced and linked on the basis of the X.509 identity certificates that they use. Identity authentication and privacy are not competing interests that need to be balanced, however. Advances in modern cryptography allow for the creation of certified user identifiers that provide users and verifiers with all the privacy and security benefits of non-certified self-generated identifiers.

More generally, modern authentication techniques such as *digital credentials* enable issuers to certify user identifiers (and, more generally, *identity assertions*) in such a manner that no tracing, linking, and impersonation powers arise in them.

Further Reading

[1] R. Clarke, "*Anonymous, Pseudonymous and Identified Transactions: The Spectrum of Choice*," Proc. IFIP User Identification & Privacy Protection Conference, Stockholm, June 1999. Available for download at http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html.

[2] The London School of Economics and Political Science, "*The Identity Project; an assessment of the UK Identity Cards Bill and its implications*,"

Version 1.09, June 27, 2005. See in particular pages 265 – 272. Available for download at http://is.lse.ac.uk/idcard/identityreport.pdf.

[3] S. Brands, "*Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*," MIT Press, ISBN 0-262-02491-8, August 2000. Available for download at http://www.credentica.com/technology/book.html.

Dr. Stefan Brands