An Overlooked Cryptographic Requirement for NSTIC

Francisco Corella, PhD
fcorella@pomcor.com

Karen Lewison, MD
kplewison@pomcor.com

September 26, 2011

Abstract

NSTIC [1] calls for the deployment of privacy-friendly (PF) credentials (based on *privacy-enhancing technologies*) on the Web. Since this has never been successfully accomplished before, it should be considered an emerging application of cryptography.

Most PF credentials are designed for issuance-show and multi-show unlinkability (with the notable exception of U-Prove, which does not provide multi-show unlinkability [2, Section 2.2]). Unfortunately that makes it impossible to revoke them using a traditional certificate revocation list (CRL). Although this is a well-known problem in cryptography, its implications for NSTIC have been overlooked.

NSTIC literature [3, 4] assumes that there exist PF credential systems ready for deployment. Government documents do not name those technologies, but they are understood to be U-Prove [5] and Idemix [6]. However, neither U-Prove nor Idemix allow the issuer of a credential to revoke it. (A U-Prove credential can be revoked by the credential *user* because of U-Prove's lack of multi-show unlinkability.) Thus they both lack a key feature of a credential system that is ordinarily taken for granted. The U-Prove documentation [7] suggests workarounds, but they seem impractical.

Several cryptographic solutions have been proposed to the revocation problem. Solutions based on accumulators [8, 9, 10, 11, 12, 13] seem impractical due to their witness-update requirement. In other solutions, the cost of showing a credential grows with the number of revocations [14, 2, 15], albeit only sublinearly

in [2]. But there is at least one solution [16] (designed for group signatures but probably adaptable to PF credentials) that has a constant show cost.

All this suggests that the technology assumptions underlying NSTIC should be revised to take into account revocation requirements, and that second-generation privacy-enhancing technologies may need to be developed.

References

[1] NSTIC National Program Office. Web site of the National Strategy for Trusted Identities in Cyberspace. At http://www.nist.gov/nstic/.

[2] S. Brands, L. Demuynck, and B. De Decker. A practical system for globally revoking the unlinkable pseudonyms of unknown users. In *Proceedings of the 12th Australasian conference on Information security and privacy*, July 2007. Pre-conference report available at http://www.cs.kuleuven.be/publicaties/rapporten/cw/CW472.pdf.

[3] Howard A. Schmidt. The National Strategy for Trusted Identities in Cyberspace and Your Privacy, April 26, 2011. White House blog post, available at http://www.whitehouse.gov/blog/2011/04/26/national-strategy-trusted-identities-cyberspace-and-your-privacy.

[4] The White House. National Strategy for Trusted Identities in Cyberspace, April 2011. Available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[5] Microsoft Corporation. U-Prove Home Page. At http://www.microsoft.com/u-prove.

[6] J. Camenisch, P. Bichsel, and T. Gross. Idemix Blog. At http://idemix.wordpress.com/.

[7] Christian Paquin. U-Prove Technology Overview V1.1 Draft Revision 1, February 2011. There is no http URL for this document, but it can be downloaded by following links from http://www.microsoft.com/u-prove.

[8] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '02, pages 61–76, London, UK, 2002. Springer-Verlag.

[9] J. Li, N. Li, and R. Xue. Universal accumulators with efficient nonmembership proofs. In *Applied Cryptography and Network Security*, pages 253–269, 2007.

[10] Man Ho Au, Patrick P. Tsang, Willy Susilo, and Yi Mu. Dynamic universal accumulators for ddh groups and their application to attribute-based anonymous credential systems. In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology*, CT-RSA '09, pages 295–308, Berlin, Heidelberg, 2009. Springer-Verlag.

[11] Lan Nguyen. Accumulators from bilinear pairings and applications. In *The Cryptographer's Track at RSA Conference*, pages 275–292, 2005.

[12] Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In *Public Key Cryptography*, pages 481–500, 2009.

[13] Tolga Acar and Lan Nguyen. Revocation for delegatable anonymous credentials. In *Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography*, PKC'11, pages 423–440, Berlin, Heidelberg, 2011. Springer-Verlag.

[14] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *Proceedings of the 11th ACM conference on Computer and communications security*, CCS '04, pages 168–177, New York, NY, USA, 2004. ACM.

[15] Patrick P. Tsang, Man Ho Au, Apu Kapadia, and Sean W. Smith. Blacklistable anonymous credentials: blocking misbehaving users without ttps. In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, pages 72–81, New York, NY, USA, 2007. ACM.

[16] Toru Nakanishi, Hiroki Fujii, Yuta Hira, and Nobuo Funabiki. Revocable group signature schemes with constant costs for signing and verifying. *Ieice Transactions*, 93-A:50–62, 2010.