Cryptology ePrint Archive: Report 2013/207

Self-blindable Credential: Towards LightWeight Anonymous Entity Authentication

Yanjiang Yang and Xuhua Ding and Haibing Lu and Jian Weng

Abstract: We are witnessing the rapid expansion of smart devices in our daily life. The need for individual privacy protection calls for anonymous entity authentication techniques with affordable efficiency upon the resource-constrained smart devices. Towards this objective, in this paper we propose self-blindable credential, a lightweight anonymous entity authentication primitive. We provide a formulation of the primitive and present two concrete instantiations. The first scheme implements verifier-local revocation and the second scheme enhances the former with forward security. Our analytical performance results show that our schemes outperform relevant existing schemes.

Category / Keywords: public-key cryptography / anonymity

Date: received 10 Apr 2013

Contact author: yyang at i2r a-star edu sg

Available formats: PDF | BibTeX Citation

Version: 20130414:152542 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]