Privacy-Enhancing Identity Ecosystem

H. Karen Lu & Laurent Castillo
Gemalto, Inc.
Karen.lu@gemalto.com, Laurent.castillo@gemalto.com

Abstract: Federated identity solutions enable cross-domain collaborations, reduce passwords management hassles, and enhance security of identity management. This achievement, however, can be at the cost of users' privacy since an identity provider can track users' behaviors. Privacy-enhancing (PE) credential systems protect users' privacy by untraceability between credential issuance and usage, unlinkability between transactions, and selective information disclosure. While the underlying cryptography is well understood, the new challenges are how to effectively integrate such technologies into an identity ecosystem. Special attention is required to add privacy not only to credentials but also to protocols, and to reach good levels of usability and user acceptance. This paper presents our work toward addressing these issues. We propose a PE identity system that integrates the PE credentials and smart card technologies, and leverages existing federated identity solutions. The paper describes the technologies for constructing the system, including building blocks, credential issuance, credential usage, secure element, and access control. The implementation and deployment challenges will lead to topics of future work.