A General Certification Framework with Applications to Privacy-Enhancing Certificate Infrastructures

Jan Camenisch, Thomas Groß, and Dieter Sommer

IBM Research, Zurich Research Laboratory

Abstract. Interactions in electronic media require mutual trust to be established, preferably through the release of certified information. Disclosing certificates for provisioning the required information often leads to the disclosure of additional information not required for the purpose of the interaction. For instance, ordinary certificates unnecessarily reveal their binary representation.
We propose a certificate-based framework comprising protocol definitions and abstract interface specifications for controlled, that is well-specified, release of data. This includes controlled release during the certification of data and controlled release of certified data. The protocols are based on proofs of knowledge of certificates and relations over the attributes, ensuring that no side information but only the specified data are revealed. Furthermore, the protocols allow one to release certified data in plain or encrypted form and to prove general expressions over the data items. Our framework can be seen as a generalization of anonymous credential systems, group signature, traceable signature, and e-cash schemes. The framework encompasses a specification language that allows one to precisely specify what data to release and how to release them in the protocols.
We outline how our framework can be implemented cryptographically. The key application of our framework is the user-controlled release of attributes. Leveraging ideas of public key infrastructures, a privacy PKI (pPKI) can be built on top of the framework. We consider our framework a central building block to achieve privacy on the Internet.

1 Introduction

In today's interactions in electronic media users are frequently required to release personally identifying information (PII). A basic principle fostered by consumer protection agencies and privacy advocates is the idea of data minimization stating that the amount of data being provided should be minimal for a given purpose. Another principle is that users should be in control of their data.

The digital world makes it easy for organizations to build extensive profiles of users based on the data they obtain in interactions. It also provides new ways of protecting the privacy of users by employing cryptography to limit the amount of data being released in an interaction following the data minization principle.

Today's infrastructures within electronic media have often not been designed to take privacy into consideration. Scalable privacy support within such infrastructures requires the availability of a privacy architecture which allows for integrating privacy principles into the infrastructures. Research efforts involving privacy architecures are currently ongoing, for example, within the European PRIME project [10]. A privacy architecture includes privacy-enhancing authorization mechanisms allowing decisions to be based on a requester's (certified) attributes rather than on her identity, and languages for requesting general (certified) statements from a party. It is likely that such privacy architectures will emerge within the next few years.

We define a general framework for data minimization allowing for precise specifications of what certified data to release to whom in a transaction and sketch the required cryptographic mechanisms. The full paper [4] gives an application of the framework to build a privacy-enhanced PKI (pPKI).

Our framework allows a party to obtain certificates while the issuer does not necessarily learn all data items being certified, but the issuer knows—through a proof performed by the party—that the party has a certificate from a particular issuer on such a data item. It furthermore allows the party to prove properties over certified data without revealing any other information, even not the certificate itself. The proofs encompass proofs of polynomial relations over certified data items and the computation of commitments and encryptions of polynomials over certified data items. The proofs allow for logical conjunction and disjunction operators over predicates on data items, encryptions, and commitments. The framework includes protocol descriptions with API definitions for obtaining certificates and proving knowledge and properties of certificates while being able to control precisely what data to release and to whom. We present a specification language for specifying this release of data.

Related Work. The research area our framework is positioned in was pioneered by Chaum who defined the concepts of credential systems, see for example [5], group signature schemes [7], and electronic cash systems [6]. Our framework can be seen as a generalization of these systems, as well as anonymous attestation schemes [3], traceable signature schemes [8] and identity escrow schemes [9]. Indeed, our framework can be instantiated to obtain a generalized anonymous credential system, a group signature scheme, traceable signature scheme, or an e-cash scheme. The pseudonym system of Brands [2] also provides efficient techniques for proving relations among committed values, but his overall construction falls short of supporting multi-show unlinkability thus restricting its applicability.

A cryptographic framework for releasing certified data has been proposed by Bangerter et al. [1]. The framework provides an initial step towards a general framework as put forth in our paper [4]. The basic idea of using signature protocols for obtaining and proving signatures remains the same, but our approach is more general with respect to several aspects. It provides much more powerful proof capabilities like the proof of disjunctions, more general predicates and more functionality with respect to verifiable encryption. Moreover, our frame-

work is more concrete in that we provide a specification language and concrete protocol interfaces close to an API-level making it ready for implementations and integration into privacy architectures and infrastructures. The high level of abstraction of our specification language allows for an easy integration into privacy architectures. The implementation of our framework is readily employable for pseudonymous authentication.

We will present our generalized framework for controlled data release including an interface specification for the protocols and the definition of a specification language and semantics for data release.

References

1. Endre Bangerter, Jan Camenisch, and Anna Lysyanskaya. A cryptographic framework for the controlled release of certified data. In *Twelfth International Workshop on Security Protocols 2004*, LNCS. Springer Verlag, 2004.
2. Stefan Brands. *Rethinking Public Key Infrastructure and Digital Certificates—Building in Privacy.* PhD thesis, Eindhoven Institute of Technology, Eindhoven, The Netherlands, 1999.
3. Ernie Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 132–145, New York, NY, USA, 2004. ACM Press.
4. Jan Camenisch, Dieter Sommer, and Roger Zimmermann. A general certification framework with applications to privacy-enhancing certificate infrastructures. Technical Report 3629, IBM Research, November 2005.
5. David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, February 1981.
6. David Chaum. Blind signature systems. In David Chaum, editor, *Advances in Cryptology — CRYPTO '83*, page 153. Plenum Press, 1984.
7. David Chaum and Eugène van Heyst. Group signatures. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, volume 547 of *LNCS*, pages 257–265. Springer-Verlag, 1991.
8. Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung. Traceable signatures. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 571–589. Springer, 2004.
9. Joe Kilian and Erez Petrank. Identity escrow. Theory of Cryptography Library, Record Nr. 97-11, `http://theory.lcs.mit.edu/~tcryptol`, August 1997.
10. PRIME project. `www.prime-project.eu.org`.