Chapter 3

A Distributed and Secure Architecture for Signature and Decryption Delegation through Remote Smart Cards

Giuseppe Cattaneo
Università di Salerno, Italy

Pompeo Faruolo
Università di Salerno, Italy

Ivan Visconti
Università di Salerno, Italy

ABSTRACT

The established legal value of digital signatures and the growing availability of identity-based digital services are progressively extending the use of smart cards to all citizens, opening new challenging scenarios. Among them, motivated by concrete applications, secure and practical delegation of digital signatures and decryptions is becoming more and more critical. Unfortunately, all secure delegation systems proposed so far include various drawbacks with respect to some of the main functional requirements of any practical system. With the purpose of proposing a truly practical solution for signature and decryption delegation, in this chapter the authors put forth the notion of a “Proxy Smart Card System,” a distributed system that allows a smart card owner to delegate part of its computations to remote users. They first stress the problematic aspects concerning the use of known proxy-cryptography schemes in synergy with current standard technologies, which in turn motivates the need of proxy smart card systems. Then they formalize the security and functional requirements of a proxy smart card system, identifying the involved parties, the adversary model, and the usability properties. Finally, the authors present the design and analysis of a proxy smart card system, which implements the required functionalities outperforming the current state of the art.

DOI: 10.4018/978-1-4666-0978-5.ch003
A Distributed and Secure Architecture for Signature and Decryption Delegation

INTRODUCTION

Proxy cryptography is a widely developed research area that consists in providing cryptographic primitives that allow a user to safely delegate part of its tasks (typically decryptions and signatures of messages) to another user. Concrete applications of proxy cryptography are nowadays becoming more and more critical.

For instance digital signatures are now regulated and accepted by law in almost all countries and many entities playing crucial roles in both enterprises (e.g., CEOs) and public institutions (e.g., mayors, rectors), have to sign a large amount of documents per day. Moreover, it is often the case that documents have to be signed urgently, even when the signer is out of his office and unreachable. The possibility of delegating signing privileges should therefore be extended also to digital signatures.

Another major example is the increasing use of decryption features for e-mails, in order to keep private some relevant data. Again, one would like to delegate to someone else the capability of decrypting some of the emails (e.g., the ones with a specific subject) in order to reduce his own amount of work and not to stop his activities when he is disconnected from the Internet.

Unfortunately we observe a huge gap between features provided by proxy cryptography and their actual use in the real world. Indeed, it is well known that results produced by cryptographers need several years to be assessed and then used by practitioners. Moreover cryptography in standalone is not usable, it needs to be integrated in a system with security and privacy mechanisms that can make robust all the involved components. Proxy cryptography is affected by such delays, and indeed, while the literature already gives several provably secure schemes enjoying many features and reasonable efficiency, almost nothing of it is actually used in practice. This is in large part a consequence of the long distance between the requirements of proxy cryptography (e.g., system parameters, cryptographic operations) and the currently used technologies (e.g., PKIX (Housley et al., 2002), Smart Cards). It is therefore urgent to provide mechanisms that allow delegation of signatures and decryptions using current standard technologies only.

Contribution

In this work we study the problematic aspects of using proxy cryptography along with current standard technologies to implement delegation of signatures and decryptions. Therefore, motivated by the worldwide spread of smart cards (SCs, for short), and their cryptographic operations (e.g., signatures and decryptions) for implementing various cryptographic services, we put forth the notion of a Proxy Smart Card System (PSCS, for short).

We investigate concrete real-world scenarios and according to them we formalize the security and functional requirements of a PSCS, identifying the involved parties, the adversary model and the critical usability properties. We finally present the design and analysis of a proxy smart card system (based on the use of a network security appliance) that outperforms the current state of the art. The development of our system required the combined use of several techniques and technologies in a novel way, which in some case could be also of independent interest.

Our solution is a “ready-to-use” framework that can be easily plugged in real-life scenarios. It does not resort to currently unused features of proxy cryptography and instead uses the synergy of existing crypto tools and security technologies to obtain a robust, easy to configure, scalable and cheap system to delegate, under some access control policies, signature and decryption privileges.

Organization of the Chapter

The chapter is organized as follows. In the next section we first briefly present the state of art of proxy signature and decryption, and then we