List of Figures

Chapter 1

Introduction

In this chapter we examine the role and the importance of digital certificates in communication and transaction mechanisms. We discuss the main developments and point out their security, efficiency, and privacy shortcomings. Next we examine the meager previous efforts to protect privacy in public key infrastructures. Amongst others, we show that the popular suggestion to offer privacy by issuing pseudonymous certificates is not only insecure in almost all situations, but also ineffective to protect privacy. On the basis of the previous findings we list basic desirable privacy properties. Finally, we outline how the techniques that will be developed in later chapters meet these and other privacy properties and at the same time help overcome the security and efficiency problems.

1.1 Digital certificates and PKIs

1.1.1 From paper-based to digital certificates

Individuals and organizations often have a legitimate need to verify the identity or other attributes of the individuals they communicate or transact with. The traditional method for demonstrating that one meets certain qualifications is to disclose one or more paper-based certificates. As defined in the third edition of the American Heritage Dictionary of the English Language, a certificate is "a document testifying to the truth of something." Photographs, handwritten signatures, and physical cues help the verifier to establish the identity of the holder of a certificate. Embedded security features (such as special paper, watermarks, ink that appears different when viewed from different angles, and microprinted words and other detail that is hard to replicate) serve to protect against counterfeiting and unauthorized duplication.

Since the advent of computers and telecommunication networks, paper-based transaction mechanisms are being replaced by electronic transaction mechanisms at

a breath-taking pace. Many forces drive this unstoppable transition:

- The theft, loss, or destruction of a paper-based certificate coincides with the theft, loss, or destruction of at least part of its value. It may be expensive, difficult, or impossible to obtain a new copy from the issuer.

- Paper-based certificates are subject to wear and tear, add to the depletion of forests, are costly to handle, and in many situations are inefficient. Electronic certificates can be manufactured, distributed, copied, verified, and processed much more efficiently and at lesser cost.

- Paper-based certificates are not suitable to convey negative qualifications of their holders. An individual carrying a certificate attesting to the fact that he or she has been in prison, say, can simply discard the certificate. Sometimes negative qualifications can be tied in with positive ones (e.g., a mark for drunk driving on a driver's license), but this measure is not always an option.

- Cyberspace (the conglomeration of networks that enable remote communication, including the Internet, e-mail, cable TV, and mobile phone networks such as GSM) offers huge benefits over face-to-face communications and transactions in the physical world. Many of the benefits cannot be realized using paper-based certificates, however, since these require physical transport.

- The public at large can avail itself at modest cost of ever-advancing desktop reprographic equipment. A nationwide study conducted in 1998 by U.S. corporate investigation firm Kessler & Associates found resume and credential fraud to be of "almost epidemic proportions." Counterfeiting rarely requires perfection; it usually suffices to produce something that will pass casual human inspection. Ultimately, the counterfeiting threat can be overcome only by moving to certificates that are cryptographically secured and that can be verified with 100 percent accuracy by computers.

In many applications, symmetric cryptographic techniques are inappropriate: they require a trusted third party to set up a secret key for any two parties that have not communicated previously, and cannot offer non-repudiation. Thus, there is a fundamental need for public key cryptography. Public key cryptography enables the parties in a system to digitally sign and encrypt their messages. When two parties that have not communicated before want to establish an authenticated session, they need merely fetch the public key of the other; there is no need for a trusted third party to mediate every transaction.

In their seminal paper [136] on public key cryptography, Diffie and Hellman pointed out the problem of authenticating that a public key belongs to an entity. They suggested using secure online repositories with entries that specify name–key bindings. In 1978, Kohnfelder [238] proposed to avoid this potential bottleneck by having