Electronic Signatures and Ethics

A. Srivastava
Monash University, Australia

S. B. Thomson
Monash University, Australia

INTRODUCTION

The advent of the Internet once again raised the question as to what constitutes a signature and what form of signature should be used to sign electronic documents. This led legal jurists and academics to examine what a signature is. Traditionally, a signature is "the name of a person written with his or her own hand" (Merriam-Webster Online Dictionary, 2006), and since 439 AD in the Roman Empire, a signature authenticated wills (Nicholas, 1965). However, courts have accepted various other forms of signature such as initials, marks, rubber stamp, typed name, and a printed name.[1] Thus the validity of a signature is not to be tested by its form but rather by the functions it performs (Reed, 2000). The primary functions of a signature are to provide evidence: (1) of the identity of the signatory, (2) that the signatory intended the signature to be his/her signature, and (3) that the signatory approves and adopts the contents of the document as his/her own (Reed, 2000). The primary functions of a signature are the only mandatory requirement adopted by most legislation for signing electronic documents.[2] Thus, any type of technology that has the ability to satisfy the primary functions of a signature can be used to sign electronic documents. Such types of technologies are generically known as *electronic signatures* (ESs).

ES is defined as "data in electronic form…affixed to or logically associated with (an electronic record)…used to identify the signatory…and indicate the signatory's approval…" (UNCITRAL MLES, 2001, Article 2a). Examples of ESs include, but are not limited to, a password, a typed name at the end of an e-mail, a personal identification number (PIN), a biometric indicator, and a digital signature (DS). Among all the types of ESs, DS is the most popular as judged by the fact that the term is often used interchangeably with ES (Shark Tank, 2003). DS is a technologically specific mechanism based on Public Key Cryptography (PKC), whereas ES is a technology-neutral term and can be any technology that is able to satisfy the legislative requirements.

The aim of this article is to describe in detail the various forms of ESs, especially DS, and analyze the ethical issues associated with the usage of ES/DS. The first section explains in detail the technology of DS, describes the legal functions that a DS performs in the electronic environment, and explains the implementation of DSs. Next we describe other forms of ESs such as passwords, PINs, "typed name at the end of e-mail," and the various forms of biometrics. The ethical issues associated with the usage of ES/DS are examined, and we end with a summary of the article.

DIGITAL SIGNATURES

DSs are formed and verified by using cryptography, the branch of applied mathematics concerned with transforming messages into seemingly incomprehensible form and back again into the original form (Electronic Frontiers, 2005). DS performs three important functions: *authentication, integrity,* and *non-repudiation. Authentication* is "broadly the act of proving that something (as a document) is true or genuine…" (Garner, 2004, p. 142). *Integrity* protects the contents of data, so that it is possible to know that the read message has not been changed either accidentally or maliciously. Non-repudiation is "a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action…" (ECEG, 1998, Appendix 4). The sender of the message cannot falsely repudiate that the message has not been sent by him/her.

The Implementation of DSs

Based upon a technologically specific mechanism, PKC, or asymmetric-key cryptography, a DS subscriber has two keys: a private key and a public key. These

key pairs are obtained from an institution known as a certification authority (CA), which associates the public and private key pair to an individual. The private key and the public key are unique to the subscriber and work as a functioning key pair. The private key is only known to the user, just like a password or PIN, whereas the public key is known to the public and can be found in a similar manner to a person's name and phone number in a telephone directory.[3] The procedure described in Diagram 1 identifies the method used to seal a document with the DS.

The data message to be sent is first hashed through a hashing algorithm to get a message digest. To the message digest the signer (user) applies his/her private key (124) to obtain a DS. After receiving the DS the sender (signer) attaches the DS to the data message. Both the attached data message and DS are encrypted with the recipient's public key (362) and sent to the recipient. Upon receipt of the digitally signed document, the receiver will separate the DS from the body of the document (data message) with his/her private key (263). The data message is then hashed using the same algorithm that the signer used to create the DS. This will result in the message digest (1). The DS is then processed using the signer's public key (421) to receive a second message digest (2). If both (1) and (2) are the same, then the recipient has verified the identity of the signer because the signer's public key will verify only a DS created with the signer's private key. The message integrity is established because the message is shown to have remained unaltered.

Even though the process shown in Figure 1 is considered as being highly secure, it is a very slow process. In reality, for maintaining the security as well as retaining high-speed data transfer, DS technology uses both a symmetric and asymmetric crypto system. Figure 2 demonstrates this process. Data is encrypted in two phases:

1. A symmetric key (123) is used to encrypt the body of message (data message + digital signature).
2. The symmetric key (123) is then encrypted with the recipient's public key and sent along with the encrypted message.

When the body of document (data message + digital signature + symmetric key (123)) reaches the recipient, the recipient decrypts the data in two phases:

1. The recipient decrypts the body of document (data message + digital signature + symmetric key (123)) through his/her private key to receive the symmetric key.
2. With the symmetric key now decrypted, the message body (data message + digital signature) can be decrypted with the help of the symmetric key (123).

The above method not only enhances the speed of data transfer but also encrypts the body of the message twice, making it doubly secure.

Figure 1. Implementation of a DS[4]