Available online at www.sciencedirect.com
SCIENCE DIRECT®
Information & Management 41 (2004) 561–575
INFORMATION & MANAGEMENT
www.elsevier.com/locate/dsw

Digital signature: use and modification to achieve success in next generational e-business processes

Alok Gupta[a,*], Y. Alex Tung[b,1], James R. Marsden[b,1]

[a]*Department of Information and Decision Sciences, Carlson School of Management, University of Minnesota, Minneapolis, MN 55455, USA*
[b]*Department of Operations and Information Management, School of Business Administration, University of Connecticut, Storrs, CT 06269, USA*

Received 1 February 2002; received in revised form 1 February 2003; accepted 1 June 2003

Abstract

A US law, the electronic signatures (E-Sign) in Global and National Commerce Act (signed by then President Clinton on 30 June 2000 with an effective date of 1 October 2000), grants electronic signatures legal validity equivalent to traditional hand-written counterparts. The intention of this law is to cut costs while providing more stringent security. In the emerging e-commerce arena, electronic signatures hold great potential for facilitating secure electronic transactions. But signatures are used in many critical business processes that occur prior to or independent of final transactions. Contract development and numerous other processes entail a series of draft modifications and sign-offs. Can electronic signatures provide cost savings and security in these activities? In this paper, we

(i) detail fundamentals and the current status of electronic signatures;
(ii) describe the integration of electronic signatures with electronic verification and authentication technologies;
(iii) explore e-commerce applications, especially document management processes, that could benefit from adopting electronic signatures; and
(iv) propose modifications to the electronic signature process to enable innovative document management processes. We propose modifications using *partial document ownership*, *soft signatures*, and *hard signatures*.

Keywords: Electronic signature; Digital signature; E-commerce; Computer verification and authentication; Biometrics technologies; Computer security; Negotiation support

1. Introduction

In the e-commerce arena, security is a great concern to many organizations when a considerable volume of documents and transactions are computerized/digitized and exchanged online [8,11,13]. This paper's primary focus is on the techniques commonly referred to as ''digital signatures,'' which are attachments to documents used to verify or authenticate a ''signer'' *and* the document signed. Combined with certificates issued by trusted third parties and enhanced by biometric authentication tools, digital signatures are gaining a presence in the transaction or final document arena. Our argument, however, is that their really

* Corresponding author. Fax: +1-612-6261316.
E-mail addresses: agupta@csom.umn.edu (A. Gupta), atung@business.uconn.edu (Y.A. Tung), jimm@business.uconn.edu (J.R. Marsden).
[1] Fax: +1-860-4864839.

0378-7206/$ – see front matter
doi:10.1016/S0378-7206(03)00090-9

significant benefits for companies and organizations lie in potential improvement of stepwise sign-off processes including negotiation and contract/document generation.

Following the American Bar Association (ABA) guidelines [1], we differentiate digital signatures from the more mundane digitized images of hand-written signatures, such as typed notations like '/s/John Smith', or even addressing notations, such as electronic mail headers. In addition to improved security, digital signatures provide the following advantages:

(i) no need to print out documents for signing;
(ii) reduced storage of paper copies;
(iii) improved management and access (anytime/anywhere) of electronic versus paper documents;
(iv) elimination of need for faxing or overnight mailing—reduction of cycle time;
(v) improved security of document transmission; and
(vi) enhanced management processes outside the ''final signature'' step.

The concepts and ideas in this paper have been developed in an attempt to adopt leading edge digital signature technologies for everyday business processes. Operational managers helped in shaping and refining the vision of an ideal system and helped identify the shortcomings/limitations of current digital signature technology. Such interaction is critically important in understanding existing practices as well as in shaping technological solutions that enabled process enhancements.

2. Concept and current status of digital signature

Digital signatures process is based on the idea of asymmetric encryption. Each user of this paradigm has two ''keys'' assigned to them. One of the keys is known only to the user and is called ''private'' key while the other key is public knowledge and is known as ''public'' key. Both *public* and *private* keys can be used to encrypt or decrypt data, however, whatever is encrypted by *public* key can only be decrypted by *private* key and vice versa. Typical encryption, for example the encryption of credit card information for online transactions, requires that the data be encrypted using recipients public key so that only intended receiver (such as Amazon.com) can decrypt the data. However, digital signature involves reverse of the encryption process. The data is encrypted with the private key of an entity and anyone can decrypt it using the public key; since a public key can only decrypt the data from a corresponding private key, the identity of the sender is verified. Since digital signatures are often used with large documents and encryption is a computationally intensive technique, instead of encrypting the document, a hash of the document is typically computed and encrypted. A hash is a unique representation of a text but typically would be much smaller in size as compared to the original document. There are a variety of asymmetric cryptosystems that create and verify digital signatures. While these use different algorithms, they share the operational pattern described above. Fig. 1 depicts the digital signature creation and verification processes.We use the term *authentication* to refer to any process through which one verifies information. One may want to verify the origin of a document, the identity of the sender, the time and date a document was sent and/or signed, the identity of a computer or user, etc. The process of verification involves the following elements:

Digital signature: Created and verified using a cryptosystem.
Private key: One part of the key used to create the digital signature; known only to the signer.
Public key: The second part of the key used to decrypt or verify the digital signature; available to all those needing to communicate with the signer or validate the document, etc.
Hash function: Algorithm used in creating a digital representation, unique to a message or document, in the form of a hash value or hash result.

The ABA guidelines provide the following summary of the digital signature process:

> To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to be signed is termed the ''message'' ... a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signer's private key. The resulting signature is thus