Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 3 Issue 9, September - 2016

DIGITAL SIGNATURES

Matthew N. O. Sadiku
Roy G. Perry College of Engineering
Prairie View A&M University, TX 77446
sadiku@ieee.org

Mahamadou Tembely
Roy G. Perry College of Engineering
Prairie View A&M University, TX 77446
mtembely@student.pvmau.edu

Sarhan M. Musa
Roy G. Perry College of Engineering
Prairie View A&M University, TX 77446
smmusa@pvamu.edu

***Abstract*— With the growing use of the Internet for business, healthcare, finance, education, and legal transactions, there is a need for secured transactions and contractual agreements. The open nature of the Internet reduces the privacy level. Digital signature may be a solution ensuring both the identity of the user and the integrity of the digital document signed by the user. The aim of this paper is to provide a brief introduction to digital signatures.**

Keywords—Digital signature, electronic signature

I. INTRODUCTION

Throughout history, we have been using written contracts to legally bind ourselves. A signature is a unique notation that indicates one's approval on a given document. Signatures are needed in most legal and financial transactions today.

The process of printing a document, signing with a pen, scanning and emailing it back to the requester is inefficient. Contract signing can be time consuming when buyer and seller are far from each other. Digital signatures are one solution to this kind of problem. When affixed to an electronic document, a digital signature approves a personal identity just as a handwritten signature. A major advantage of digital signature over handwritten signatures is their security. Unlike written signatures, a digital signature is specific to the document that is signed and cannot be transferred to another document.

An electronic signature is a broader term which defines any signature in electronic form. It refers to any type of digital marking used to authenticate the writer's intent [1]. Technologies like biometrics, smart cards, and retinal scanning all fall into this category. For example, by clicking "I agree" online on a purchase form, an airline's consumer has formed a legally binding electronic signature.

Digital signatures are a subset of electronic signatures and they are created with special technology. (Not all electronic signatures are digital signatures.) They have three main roles [2]: ensure that only the intended recipients have access to the document, ensure that the document has not been altered, and ensure that the particular sender actually sent the document. Any changes made to the signed document invalidate the signature. This protects against tampering or forgery.

II. TECHNOLOGY

The technology to create secure digital signatures is proven. A digital signature is a mathematical technique for validating the authenticity and integrity of a message or document. This technique provides the highest levels of security and universal acceptance. It is used in various fields such as banking, sales, purchases, and image authentication. The most common form of digital signature involves three steps [2]: mathematical algorithms, encryption, and certification. These steps are defined in Digital Signature Standard (DSS), which was adopted in 1994 by the US government. Besides DSS, other digital signature algorithms include Rivest Shamir Adalman (RSA) algorithm, the elliptic curve variant of DSA known as the ECDSA, and Rabin signature algorithm. A digital signature is based on these asymmetric cryptographies, where each user has a pair of private and public keys. The private key is kept confidential by its owner. The public key is made available to those who need to decode the message. The private key generates signature from document hash, while the public key verifies the signature. Current standards for private/public keys are typically 128 bits. Figure 1 provides a simplified view of the digital signature process [3].

A digital signature allows the creator of the message to attach an encrypted or mathematically scrambled coded message which acts as a signature. This coded message uniquely identifies the sender. The key services that digital signatures provide include authentication, non-repudiation, and integrity. Digital signature providers follow a specific protocol called Public Key Infrastructure (PKI). Such providers include SIGNNOW, SIGNEASY, DOCUSIGN, VERISIGN, OPENTRUST, and PDF READER. They make it easy to electronically sign a document.

Digital signature is not 100% reliable and has some disadvantages [4]. Intelligent hackers can forge digital signatures and attackers can create fake signatures. Many digital signature schemes are not

compatible with each other, making it hard to share signed documents.

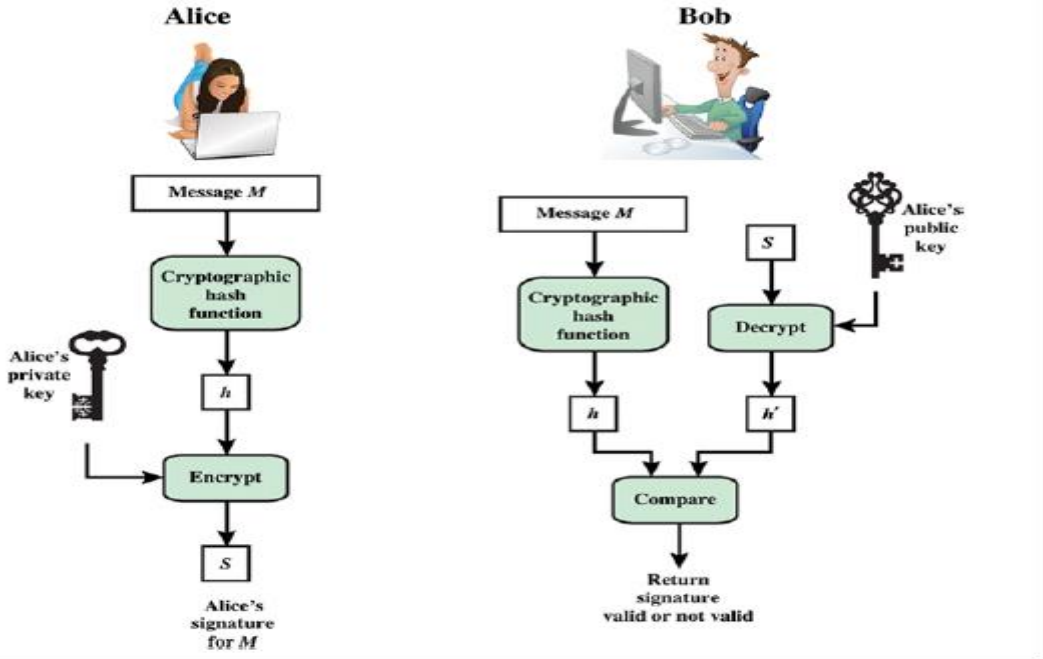

Figure 1. A simplified view of the digital signature process [3].

III. LEGAL REQUIREMENTS

The issues restraining widespread use of digital signatures are mainly legal. If you do business internationally, you expose yourself to overseas litigation. In 1999, the European Commission passed the "EU Directive for Electronic Signatures." On June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) effective on October 1, 2000. E-SIGN grants electronic signatures the same legal validity as the handwritten signatures. It allowed individual states in the U.S. to enact their own laws. After October 1, digital signatures were legally binding on a national level just as paper-based contracts. Customers could buy their cars right from home without the need to go to the car dealer to sign a credit application. Similarly, they can carry out their banking transactions and shopping needs without leaving their homes using the Internet [5].

IV. CONCLUSIONS

Digital signatures play a crucial role in communication in the digital era, as many valuable messages, documents, and images are transmitted digitally. Vendors and customers appreciate the convenience and effectiveness of conducting business online. With e-commerce booming, online transactions are multiplying and digital signatures are gradually becoming important. Digital signatures are required in e-commerce, e-banking, and e-government. They are not just for Americans. Several nations have adopted their own laws governing digital signatures. Business around the world is using digital signatures to replace the traditional pen and ink signatures. Times have changed, and business transactions are changing as well. Time will tell which direction digital signatures will take.

.

REFERENCES

[1] E H. Freeman, "Digital signatures and electronic contracts," *Information Systems Security*, vol. 13, no. 2, 2004, pp. 8-12.

[2] D. V. Borasky, "Digital signatures: Secure transactions or standards mess?" *Online*, vol. 23, no. 4, July/Aug. 1999, pp. 47-50.

[3] W. Stallings, "Digital signature algorithms," *Cryptologia*, vol. 37, no. 4, 2013, pp. 311-327.

[4] A. Doegar and M. Sivasanker, "On-demand digital signature schemes using multivariate polynomial systems," *Proceeding of International Conference on Control, Instrumentation, Communication and Computational Technologies*, 2015, pp. 393-395.

[5] B. Largent, V. C. Rogers, and T. A. March, "Digital Signatures," *Journal of Internet Commerce*,vol. 1,no.1,2002, pp. 65-73.

About the authors

Matthew N.O. Sadiku (sadiku@ieee.org) is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Mahamadou Tembely (mtembely@student.pvamu.edu) is a Ph.D student at Prairie View A&M University, Texas. He received the 2014 Outstanding MS Graduated Student award for the department of electrical and computer engineering. He is the author of several papers.

Sarhan M. Musa (smmusa@pvamu.edu) is an associate professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.