Chapter 7
Applications of Digital Signature Certificates for Online Information Security

Mohammad Tariq Banday
University of Kashmir, India

ABSTRACT

Information security has been the focus of research since decades; however, with the advent of Internet and its vast growth, online information security research has become recurrent. Novel methods, techniques, protocols, and procedures are continuously developed to secure information from growing threats. Digital signature certificates, currently offers one of the most trusted solutions to achieve CIA-trio for online information. This chapter discusses online information security through cryptography. It explains digital signature certificates; their benefits, the underlying standards, involved techniques, procedures, algorithms, processes, structure, management, formats, and illustration of their working. It highlights the potential of digital signatures and certificates in information security across different devices, services, and applications. It introduces a few useful tools to learn, train, and implement digital signature certificates.

INTRODUCTION

With the advent of digital storage and communication technologies the entire spectrum of storage and communication system has been revolutionized as digital information can be easily stored, copied, changed, and transported. More and more people and organizations are using digital documents instead of paper documents to conduct day-to-day transactions. These desirable properties of digital information are very useful but owing to easy and almost undetected modification of digital data, they have raised several security concerns. Therefore, digital data is regarded as unreliable in areas where privacy, authentication, and integrity of data are of concern unless some security procedure is attached to it. These are areas like contracts, receipts, approvals and others where users have severe and genuine concerns of unauthorized modification or disclosure of data. Hand signatures do not change this situation, because

DOI: 10.4018/978-1-4666-9426-2.ch007

it is easy to transfer a hand signature from one digitized document to another or to modify a digitized document that is hand signed. The risk of data misuse has increased many folds with the advent of networking and wireless communication as many users can gain access to the data if not secured. A solution to all these issues is digital signature. A digital signature is not a digitized hand signature, but a special kind of check-sum. Secret information ensures that a digital signature cannot be forged, while public information enables the verification of the signature. Digital signature ensures prevention of unauthorized access to data while ensuring accurate authentication to data without interference.

Different forms of encryption techniques are being used to ensure privacy of data transmitted over Internet. In addition to encryption, a digital signature of the message can be created and send along with the message by the sender. A digital signature is a checksum produced by a cryptographic transformation of data by the message sender to bind message data to the sender's identity. When properly implemented, it provides mechanisms to authenticate originator, verify data integrity, and permit signatory non-repudiation. A digital signature is an electronic, encrypted, stamp of authentication on digital information such as e-mail messages, macros, or electronic documents. A signature confirms that the information has originated from the signer and it has not been altered. Encryption and digital signature ensure information security but it is difficult to distribute and manage keys for systems that are large, heterogeneous, and geographically distributed. Public key infrastructure permits such systems to take advantages of encryption and digital signature through digital signature certificates. A digital signature certificate such as standard ITU-T X.509 certificate is a data structure signed by some trusted certification authority that binds a public key to a person, device, program, process, e-mail address, etc. Diverse types of digital signature certificates such as general purpose personal certificates, personal and enterprise e-mail certificates, SSL certificates, SSL wildcard certificates, SSL multi-domain certificates, code signing certificates, mobile device and App certificates, citizen eID and ePassports, etc. on servers, desktops, mobiles and other devices are used to secure data of various applications, services and access to devices. In addition, certificate management and certificate discovery services are used for PKI management. In addition, trusted time stamping services are integrated within digital signature certificates to authenticate time of creation of digital data. Digital signatures and digital signature certificates have tremendous prospectus and applications for information security in the era of Internet and mobility.

INFORMATION SECURITY

The term information security as defined by the US Code (2012) means "*protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (a) integrity*, *which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (b) confidentiality*, *which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (c) availability*, *which means ensuring timely and reliable access to and use of information"*. In recent years, the scope and dimensions of information security has evolved significantly. The area of information security besides covering security of data and information extends to security of networks and allied infrastructure. It has emerged as a profession across hardware, software and communication technologies for securing applications, databases and websites; security testing; information systems auditing; business continuity planning; digital forensics and crime investigations; network, and web penetration testing; incident responding; security architec-