Chapter 6

Efficient Implementation of Digital Signature Algorithms

Sumathi Doraikannan
Malla Reddy Engineering College, India

ABSTRACT

Digital Signature is considered as an authentication tool of electronic records. The main benefits of the digital signature are cost, security, time stamping, non-repudiation and speed. Digital signature can be particularly useful for sales proposals, purchase orders and health services. In addition, this chapter also focuses on the real time applications of digital signature algorithm and its implementations. This chapter deals with the Digital signature algorithm, Digital Signature types and the way of working.

INTRODUCTION

This chapter deals with the Digital signature algorithm. Digital Signature is considered as an authentication tool of electronic records. Many situations might arise where there is no trust between the sender and receiver, and something more than authentication is needed. A digital signature has the same function as the hand-written signature. Digital signatures are used to detect whether any modifications are made in the document. It enables the recipient of the information to verify the sender’s authentication and also it checks whether the information is unflawed. In addition, digital signature provides non-repudiation. Non-repudiation refers to the ability of ensuring that the sender will not deny the authenticity of their signature on a document. Thus, digital signature provides data integrity, non-repudiation and authentication. Suppose, if a branch office of any bank is in need of changing the balance of an account, the message will be sent to the head office. The head office person has to check for the authenticity of the message. If it is not proved, then the information is treated as it emerges from the unreliable source. First, this chapter presents the issues related to the digital signatures. The authors have discussed about the types of digital signatures, and its applications. Digital Signatures are an application of asymmetric cryptography.

Conventional HAND-WRITTEN signature is used to authorize a document and it is included in the document as a part of it. Digital Signatures is used to automate the signatures in a reliable way. Using
digital signatures eliminates the cost reduction and improves the speed of production processes. Digital signature can be particularly useful for sales proposals, purchase orders and health services etc. The properties of digital signature are

1. Digital signatures could be relatively easy produced.
2. Verifying and recognizing digital signature algorithm is easy.
3. Information used by the digital signature will be unique to the sender in order to prevent forgery and denial of service.

Advantages and disadvantages of digital signature are as follows:
The main benefits of the digital signature are cost, security, time stamping, non-repudiation and speed etc.

Disadvantages of digital signature are

1. Senders and receivers must buy digital certificates from trusted certification authorities.
2. Compatibility of the digital signatures plays an important role and it leads in the complication of sharing the digitally signed documents.

Digital Signature algorithm works in three steps

1. Key generation algorithm is used to generate the keys which are used to sign the document.
2. Signature generation algorithm is used for generating the signatures.
3. Verification algorithm which produces the output as accepts or rejects the signature.

The digital signature is classified based on the usage of key system. There are two key systems used for signing. 1) Private key system 2) Public key system. RSA named after Rivest, Shamir and Aldeman and Digital Signature Algorithm (DSA) use the public key system. Public key system based digital signatures have more advantages than the private-key system based digital signatures.

HISTORY OF DIGITAL SIGNATURE

Nowadays transactions and activities that take place over the Internet needs a lot of protection against various malicious activities. Out of various concerns, security plays a vital role during information transmission. Various schemes like cryptographic systems, digital Signatures were implemented in order to secure the information transmission system. A system has to be deployed for binding the documents electronically since the financial activities, business transactions grow in number nowadays. Digital signatures play the vital role in such bindings. Let us see some of the Milestones in the history of digital signature as show in Figure 1.