Cross Document Sharing using Cryptography

Mrunal Gund 1, Sakshi Marne 2, Pranita Dhamale 3, Piyush Mankar 4

[1,2,3,4] *Department of Computer Technology, Ekalavya Shikshan Sanstha's Polytechnic Pune, Maharashtra, India*

Abstract

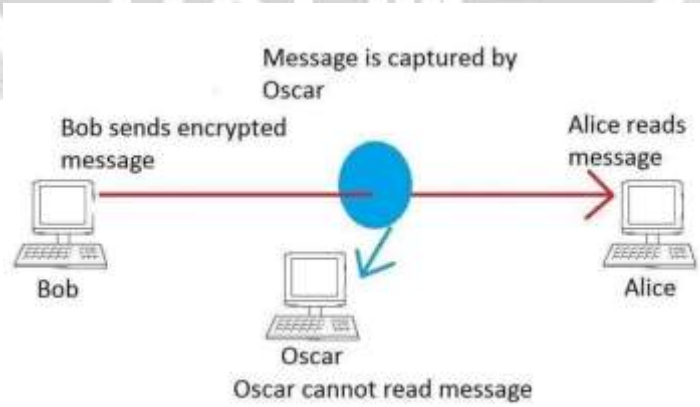
A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. This indeed is so commonly observed now in internet transactions. A digital signature can be used with any kind of message, transactions and the like, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document. Digital Signature of a person varies from document to document thus ensuring authenticity of each word of that document. As the public key of the signer is known, anybody can verify the message and the digital signature.

Keywords- *XDS document sharing, Digital Signature, Digital Signature Certificate, Encryption.*

---

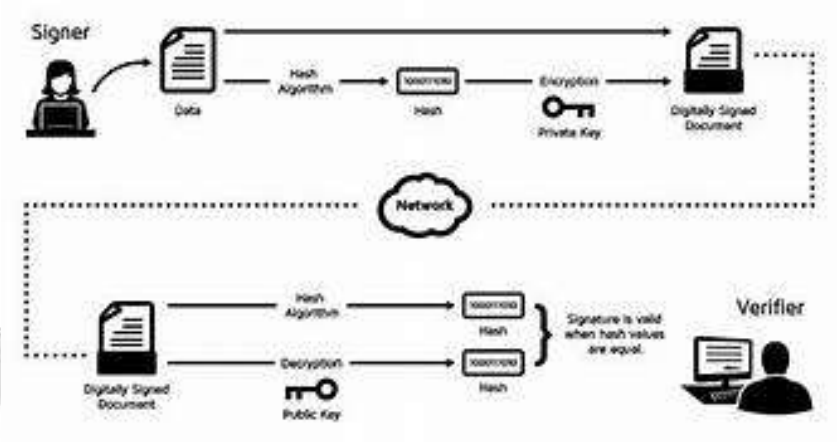
1. Introduction

Cryptography is one best technology that has made giant effect in protecting data and information in recent years. It is the science of securing your information by means ofa code. Cryptography provides an encryption for the data and information that passesvia single/multiple channels. This is done to keep the data from any external or third-party influence.



2. Digital signature

Digital signature is one of the kinds of encrypting your signature that is specific toyou and saves it from forgery of any kind. A digital signature or e-signature for short is an electronic signature that can be utilized to authenticate the identity of the sender of a message or the signer of a document.
Digital signature follows a specific protocol, called PKI (Public Key Infrastructure).
To protect the integrity of the signature, PKI requires that the keys be created, conducted, and saved in a secure manner, and often requires the services of a reliable Digital Signature Certificate.



3. Digital Certificate

A digital certificate contains identifiable information, such as a user's name, company, or department and a device's Internet Protocol (IP) address or serial number. Digital certificates contain a copy of a public key from the certificate holder, which needs to be matched to a corresponding private key to verify it is real. A public key certificate is issued by certificate authorities (CAs), which sign certificates to verify the identity of the requesting device or user.

4. Cross Sharing Document

In the field of electronic health records (EHR), Cross Enterprise Document Sharing (XDS) is a system of standards for cataloguing and sharing patient records across health institutions.[1]
XDS provides a registry for querying which patient records are in an EHR repository and methods for retrieving the documents. The XDS system of registry and repository is termed an integration profile and was created by Integrating the Healthcare Enterprise.[2] XDS uses structured EHR standards such as Continuity of Care Record (CCR) and Clinical Data Architecture (CDA) to facilitate data exchange.[2]The registry stores metadata about each document stored in a repository, including its source or location.[3] There may be multiple repositories of documents indexed,[4] but only one registry per clinical domain. XDS provides a Patient Identity Service for cross-referencing patients across multiple domains

5. Purpose

- ✓ *To provide Authenticity, Integrity and Non-repudiation to electronic documents.*
- ✓ *To use the Internet as thesafe and secure medium for e-Commerce ande - Governance.*
- ✓ *Providing accountability.*
- ✓ *Providing document integrity.*
- ✓ *Providing non-repudiation.*
- ✓ *Providing satisfactory evidence of : Authorship, Approval, Review, and Authentication.*
- ✓ *Infrastructural pattern to be further profiled by domain specific groups (e-Prescribing, e-Referral).*

6. Scope

- ✓ *A Digital Signature is an XDS document (Cross Document Sharing)*
- ✓ *The creation of a digital signature.*
- ✓ *The augmentation of a digital signature.*
- ✓ *The validation of a digital signature.*
- ✓ *Profiles associated to each form of the digital signature.*
- ✓ *Trust management.*

Out of Scope

- ✓ *Certificate management.*
- ✓ *Standards and implementations are available.*
- ✓ *Focus begins with signing, not encryption.*
- ✓ *Partial Document Signature*

7. Study of an Existing System

7.1 Verification Method

For a conventional signature, when the recipient receives a document, he/shecompares the signature on the document with the signature on file.

7.2 Relationship

For a conventional signature, there is normally a one-to-many relationship between asignature and documents.

7.3 Duplicity

In conventional signature, a copy of the signed document can be distinguished fromthe original one on file.

8. Proposed System

The aim of the proposed system is to develop a system of improved facilities. The proposed system can overcome all the limitations of the existing system. The system provides proper security and reduces the manual work.

- ✓ *The main aim of proposed system is to provide Authenticity, Integrity and Non -repudiation to electronic documents*
- ✓ *To use the Internet as the safe and secure medium for e-Commerce and e-Governance*
- ✓ *Providing accountability*
- ✓ *Providing document integrity*
- ✓ *Providing non-repudiation*
- ✓ *Providing satisfactory evidence of: Authorship, Approval, Review, andAuthentication*
- ✓ *For a digital signature, there is a one-to-one relationship between a signature and amessage.*

9. Requirements

9.1 Software Requirements

Software	***Description***
Windows	*Operating System*
Python Editor – Jupyter Notebook	*For execution of the program*

9.2 Hardware Requirements

Hardware	***Description***
Ram	*256MB*
Hard Disk	*20 GB*
Processor	*Pentium III*
Monitor	*14.4”*
Keyboard	*104 Keys*

10 Conclusion

The new communication system and digital technology has made a dramatic change inthe way in which the people transact with each other. Nowadays businessmen and consumers are using the computers to create, transmit and store the information in the electronic form instead of traditional paper documents. The information stored data in electronic form has many advantage like store, retrieve and speedier to communicate. Though the consumers are aware of these advantages, they are reluctant to conduct business or conclude any electronic transaction in the electronic form due to lack of appropriate legal framework.

Digital signature is a very effective way of securing all your financial transactions so that you will experience more convenience in terms of doing various business and money matters. This way you will not worry and go with the problems of the traditional transactions that use signatures.Digital Signature, concept of Digital Signature Certificate and what are the various contents of the digital signature certificates.

11 Acknowledgement

*We would like to pay a great thanks to our institution and a special one to our guide **Ms. Vishakha Dilpak** without whose extent support, we would never have been able to complete my seminar report.*

1.Mrunal Gund
2.Sakshi Marne
3.Pranita Dhamale
4.Piyush Mankar

Dept: Computer Science

12 Bibliography

12.1 Articles

•*Element of Applied cryptography Digital Signature by" Gainluca Dini" AnIntroduction to Cryptography and digital signature by "Ian Curry"*
•*An Introduction to and digital signature by "Asian Schools of Cyber Law".*

12.2 Websites

•*https://www.pandadoc.com/electronic-signatures/*

•*https://www.docusign.com/esignature/definition-electronic-signature-software*

•*https://www.tutorialspoint.com/information_security_cyber_law/digital_and_electroni c_signatures.html*
•*http://www.legalservicesindia.com/article/article/electronic-signature-legal- andtechnical-aspect-1827-1.html*