*Page 5609 - 5622* **DOI:** *https://doij.org/10.10000/IJLMH.111162*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 4 | Issue 3**

**2021**

# Digital Signature

HARSHITA SINGH[1]

## ABSTRACT

*Online trading is becoming more popular every day, making safety the primary issue while dealing electronically. The Digital Signature approach is important for securing transactions over open networks. It can be used in a variety of ways to secure the integrity of data sent or saved, as well as to prove the originator's identity to the recipient.*

*When transferring data, the user must ensure that the original data is not tampered with in the process of moving it from sender to receiver. In order to assure security and avoid fraud, it has also become necessary to authenticate users on a regular basis. There are many various methods of online identification, with digital signatures being one of the most powerful.*

*A study is conducted in this paper to determine the use of digital signatures and people's attitudes toward them in developed and developing countries.*

***Keywords:*** *Digital signature, Cryptography, Authentication, Public Key Cryptography, RSA, MD5.*

## I. INTRODUCTION

For a fast growing digital environment Online authentication has become necessary.Digital Signature is the best method to authenticate out of all the present methods. Digital signature not only authenticates the person, who sends the data, also ensures the integrity of the data transferred, making sure that the data has not been tampered while it is transferred. Digital signature has become a powerful tool which helps in e-filing, transactions etc.

Compared to physical signatures, Digital Signatures are much more secure and "fool-proof". Physical signatures are easily replicated or "forged". The algorithm behind digital signatures is difficult so that it is impossible to forge them. As a result of the higher security connected with Digital Signatures and the numerous points of interest connected with putting away reports electronically (rather than paper), governments in numerous nations have passed laws and regulations empowering (and now and again ordering) the utilization of digitally marked electronic archives rather than paper documents. In India the Income Tax returns or corporate returns are now uploaded electronically. A Digital Signature is a sequence of „bytes" or a code

[1] Author is a student at ABESIT Ghaziabad, India.

 [ISSN 2581-5369]

that possesses some special characteristics. A code generated is unique for a particular document by a particular signer. A different signer cannot generate an identical code for the same document or by the same signer for another document.

The awareness and percentage of people using digital signature also varies between countries. In developing countries, the percentage of internet users is very less when compared to the developed countries, which is directly proportional to the users of digital signatures. So to know about the users of digital signature in different countries, and when & where the digital signature is used in different countries, a study is carried out by dividing the countries into developed and developing countries. Doing a comparative study between them helps us to get a more clear view of the knowledge about digital signatures in different countries.

### (A) Literature Review

According to Hart (1998), "literature review is a collection of available documents on relevant topics which may be either published or unpublished. Literature review includes data, information, ideas and evidence which have been taken from a definite viewpoint of the specific topic. The viewpoint should have a certain aim and it should give the idea about how the topic will be investigated".

The knowledge about the history of digital signatures and the theoretical background of digital signature and digital signature laws of Sweden and India are collected through trustable journals. To gain data about where digital signatures are used, trustable websites were used.

## II. THEORETICAL BACKGROUND

Asymmetric cryptography and RSA algorithm are the two concepts behind the idea of Digital Signatures.

### (A) Cryptography

Cryptography is an art of transferring data from one point to another in a form that the third party can't understand. The data can be in any form. Cryptography is done by following two basic steps encryption and decryption.

### (B) RSA Algorithm

RSA, named for Ronald Rivest, Adi Shamir, and Leonard Adleman, the developers of the algorithm, is the best known of all the public key algorithms.

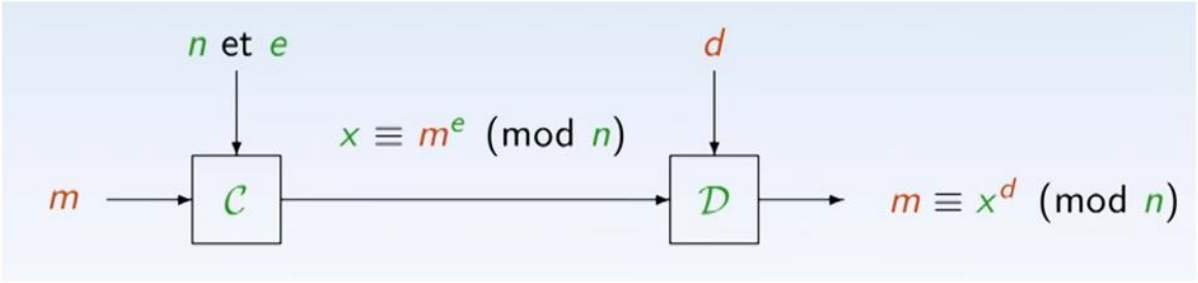
RSA algorithm is used in two important ideas, Public key encryption and digital signature. This algorithm is considered to be one of the most secure algorithms because it uses large integers

 [ISSN 2581-5369]

as the keys to perform the encryption and decryption, usually a product of two large prime numbers which is 1024 bit, approximately 300 digits, long. It takes years to find the factors that make it more secure.

The RSA algorithm is done by three steps:

- Key generation,
- Encryption and
- Decryption.




| Key Generation | |
|---|---|
| Select $p, q$ | $p$ and $q$ both prime |
| Calculate $n$ | $n = p \times q$ |
| Select integer $d$ | $gcd(\phi(n), d) = 1; 1 < d < \phi(n)$ |
| Calculate $e$ | $e = d^{-1} \bmod \phi(n)$ |
| Public Key | KU = $\{e, n\}$ |
| Private Key | KR = $\{d, n\}$ |

| Encryption |
|---|
| Plaintext: $M < n$ |
| Ciphertext: $C = M^e \pmod n$ |

| Decryption |
|---|
| Ciphertext: C |
| Plaintext: $M = C^d \pmod n$ |

**(C) Digital Signature**

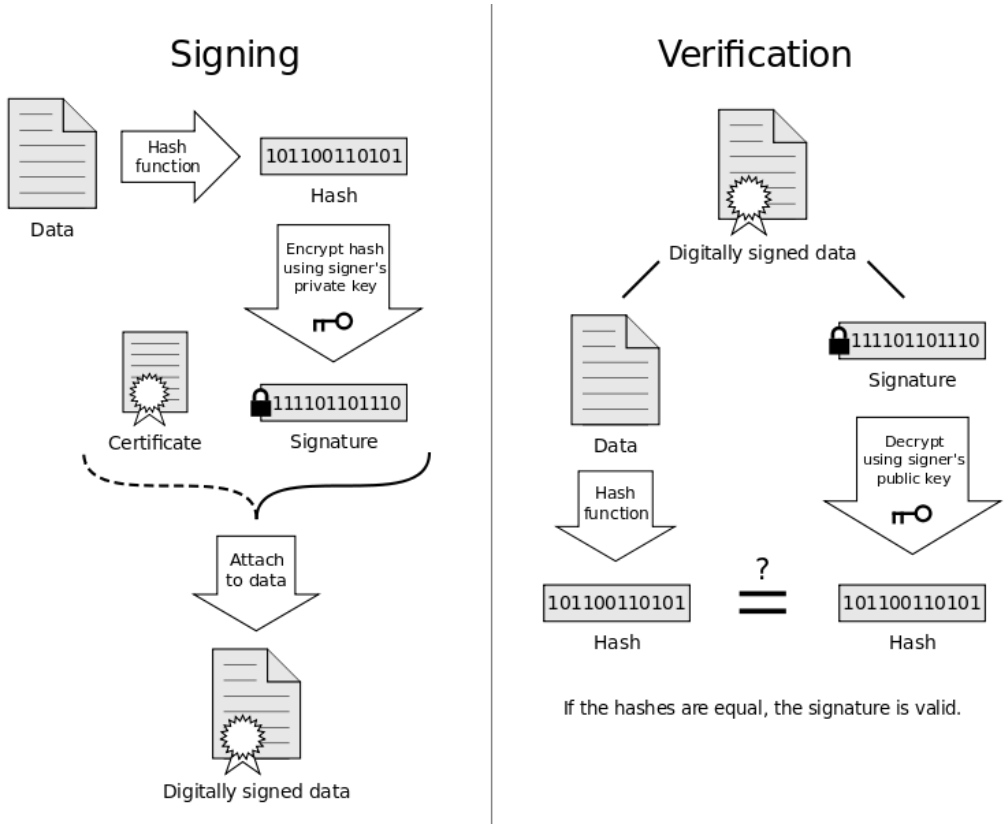
Digital Signature is a cryptographic primitive which is fundamental in authentication, authorization and nonrepudiation.

Digital signature of the digital certificate- issuing authority is also included in the digital certificate, so it is possible to check the originality of the certificate by anyone. Digital signature has the same value as the physical signature on paper. It uses asymmetric cryptography to encrypt the data, providing reason to believe that the data was send by the claimed sender.

The digital signature provides four main characters for the data sent. They are:

- **Authentication:** It means that the sender is who he/she claims to be i.e their identity can be verified.
- **Integrity:** It assures that the documents were not manipulated, altered or tampered with after they were signed.
- **Non - repudiation**: It means that after signature the person can't deny it.

**1. Signing and Verification in Digital signature**




- Signature is generated at the sender's side. First the sender will pass the document through a hash function which will generate a hash value for the document.
- Now the sender will encrypt the generated hash value using a private key. Now after that sender will attach the signature (encrypted hash value) to the original message and will send.
- Now verification happens at the receiver's side. When the receiver receives the document and using the hash function he will convert the original document into hash value and decrypts the signature using the sender's public key.
- If the hash value generated after decryption is equal to the hash value of the document then the document in valid and not manipulated.

## III. DIGITAL SIGNATURE IN SWEDEN

### (A) History

After the UNCITRAL model law on electronic commerce in 1996, the European Union passed the European Directives in 1999. Sweden's EU Presidency in 2001 was discussing with different agencies to provide "24 hour service" to its citizens and to make changes in the law that treats the electronic signature equal to the physical signature.

Swedish bank consortium was formed and major Swedish banks participated. The consortium was formed to come up with a standard structure of e-id, that fulfills the government requirements and is also easy to use by the people. As a result of the consortium, Financial IDTeknik BID AB was formed in September 2002 to create and distribute the digital signature BankID. In 2003, the first e-id was issued. 27000 people used BankID to file their tax return that year, the number crossed 100 000 during 2004 and 500 000 during May 2005. Tax and social insurance are quick to adapt the usage of digital signature (Bankid, 2013).

Initial three issuers of e-id in Sweden were BankID, Nordea and Telia. In 2007, Synovate conducted a survey on 1200 people, for Financial ID Technology, showed that 95% of the people have knowledge about BankID and e-id. In January 2008, SEB buys 18.3% of the financial identification technique's stock, became one of the largest stock holders, and started issuing the BankID to its customer.

### (B) Law on e-signature in Sweden

After the European Directives in 1999, the Qualified Electronic Signatures Act (2000:832) was passed in Sweden that made the electronic signature a rational authentication id. That is, the agreements and documents signed by digital signature are legally strong as the physical signature of a traditional contract (The agreement Title deeds and Wills are not included).[2]The laws like Consumer Credit Act, Companies Act also permit digital signature. The Money Laundry Act (2009:62) also accepts the digital signature. (Ministry of Transport and Communications 1998).

### (C) Digital signature certificate providers in Sweden

- BankID
- Nordea bank
- Telia
- Danske bank

- Handel's bank
- Skandia bank
- Länsförsäkringar
- Ikano bank
- Sparbanken öresund
- Sparbanken Syd
- Swedbank
- SEB bank
- Ica bank

**(D) Requirements to obtain a digital certificate**

Anybody who needs a digital certificate needs to have a phone number that is registered in Sweden. The age limit differs from those who have e-services and publishers. For example, you have to be at least 18 for the tax board.

A company or an organisation can't have its own digital signature, it must belong to a person and the person must have a Swedish personal identity. If an organization uses digital signature then the digital signature of the CEO or the person-in-charge is used.

| | BankID on file | BankID on cards | Id card with BankID | Mobile BankID |
|---|---|---|---|---|
| Certificate | From 18 years | From 13 years | From 13 years | From 18 years |
| Customers without Swedish personal | No | No | No | No |
| Customers with protected identity | No | Yes | Yes | No |
| Customers without official address * | Yes | No | No | No |
| Validity | 1 year | 5 years | 5 years | 3 years |
| Ordered | Internet bank | Branch | Branch | Internet Bank and Branch |

**(E) Applications of Digital Certificates in Sweden**

Digital signatures in sweden are used for many different purposes. Some of the applications

are listed below:

1. Insurance: plan retirement apply and for parental leave
2. CSN: apply for a student loan.
3. Tax: tax returns, check the tax account and print a birth certificate.
4. Swedish Change of Address: makes notification of removal.
5. Savings banks' internet banking: For carrying out secure web-based transactions and also to recognize other participants of web-based transactions
6. Direct Payment service: with Mobile BankID and BankID short, you can complete the purchase of around 500 different e-commerce sites.
7. In some agencies, you may have to look, for example, be able to represent your business. Contact each company / agency to get the proper permissions.
8. For signing documents like MS Word, MS Excel and PDFs.
9. For sending and receiving digitally signed and encrypted emails.
10. For carrying out secure web-based transactions and also to recognize other participants of web-based transactions.

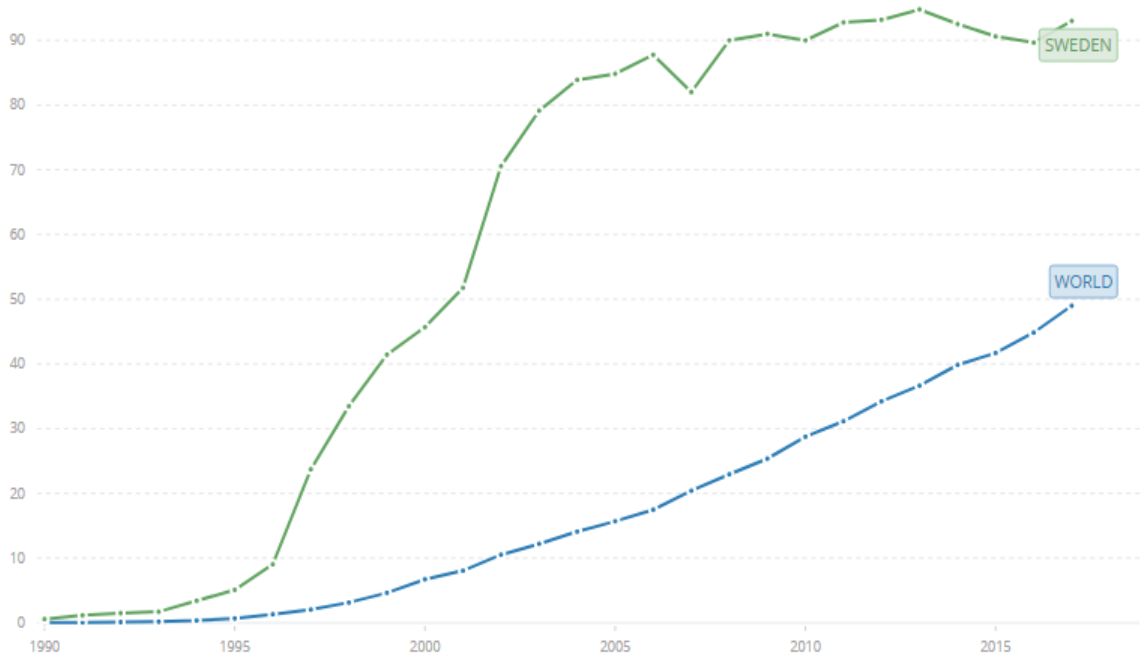
**(F) Internet users in Sweden**

Digital signature users are proportional to the internet users. The below Graph was taken from the **world development indicator**. By observing the below graph we see that more than 50% of the population in Sweden used the internet in 2001. By 2007 it was around 82%. These percentages of internet users kept on increasing and by 2015 more than 90% of the population was using the internet which jumped to 94% in 2019.

In Sweden the percentage of internet users attained a near saturation point.

**Individuals using the Internet (% of population) (1990-2019)**

 [ISSN 2581-5369]




## IV. DIGITAL SIGNATURE IN INDIA

### (A) History

E-authentication is legalized in India by passing the Information technology act 2000. The digital signatures are treated with the same legal value with the handwritten signatures and the electronic documents that have been digitally signed as same legal values as a regular paper documents. Information technology act based on asymmetric crypto system provides the required legal sanctity to the digital signatures.

The Controller of Certifying Authorities (CCA) was appointed by the central government to provide e-authentication certificates. The CCA is issuing certificates since November 1, 2000 aiming to promote the growth of E-Commerce and E- Governance. (IT Act, 2000).

### (B) Laws on e-authentication in India

The Information Technology act 2000 was passed in India based on Model Law for e-commerce proposed by UNCITRAL, with the major concepts like

- Legal recognition of data messages,
- Writing Signature,
- Original, Admissibility and evidential weight of data message,
- Formation and validity of contracts,
- Recognition of parties by data message,

 [ISSN 2581-5369]

- Acknowledgement of receipt,
- Time and dispatch and receipt of messages.

The Controller of Certifying Authorities (CCA) is appointed by the Indian central government under section 17 of the Act. The IT Act gives the CCA the jurisdiction to provide a license to Certifying Authorities CA. The CA then distributes the digital signature certificate to the general public following a set of criteria.

The digital signature of the CCA is also included in every public key of the digital signature certificate issued as established under section 18(b) of the IT act. This helps to verify the originality of the certificate. (IT Act, 2000).

**(C) Certifying Authorities**

In India, the office of the Controller of Certification Agencies (CCA) appoints certification agencies under the requirements of the Information Technology Act of 2000. The CCA has authorised a total of seven Certification Agencies to issue Digital Signature Certificates. (www.cca.gov.in).

The name of all the seven certification agencies to issue digital signature certificates are given below:

| Name of the Certifying Agency | Website Info |
|---|---|
| Tata Consultancy Services Ltd. | http://www.tcs-ca.tcs.co.in/ |
| National Informatics Centre | http://www.nic.in/ |
| Institute for Development & Research in Banking Technology (IDRBT) | idrbtca.org.in |
| MTNL | http://www.mtnltrustline.com |
| Customs & Central Excise | icert.gov.in |
| (n)Code Solutions Ltd. (A division of Gujarat Narmada Valley Fertilisers Company Ltd.) | http://www.gnvfc.com/ |
| Safescrypt | http://www.safescrypt.com/ |

**(D) Applications of Digital Certificates in India**

- To send and receive digitally signed and encrypted emails;

- to conduct secure web-based transactions; and to identify other web-based transaction participants.
- Tendering for various government projects using eTendering.
- eProcurement - Purchasing different types of commodities through eCommerce software.
- The Ministry of Corporate Affairs is responsible for registering corporations.
- eFiling – Electronic filing of income tax returns for the government.
- For signing MSWord, MSExcel, and PDF documents.

**1. Digital Signature in Filing Income Tax Returns in India**

In India, the most common application of digital signatures is for the filing of income tax returns. The following is a case study of income tax returns filed electronically

The Income Tax Rules are detailed in below Table (taken from IRT e-filing, 2013). Appropriate receipt of From 2011 to July 2013, e-Returns were used. This provides detailed information on the number of people who used digital signatures for e-filing different types of tax returns. (IRT e-filing, 2013)

| S.No. | Form | FY 2011-12 (From 01/04/2011 to 31/03/2012) | FY 2012-13 (From 01/04/2012 to 31/03/2013) | FY 2013-14 (From 01/04/2013 to 31/07/2013) |
|---|---|---|---|---|
| 1 | ITR-1 | 4439001 | 6409881 | 5781252 |
| 2 | ITR-2 | 1773659 | 2240995 | 1479280 |
| 3 | ITR-3 | 522579 | 625890 | 100646 |
| 4 | ITR-4 | 6712032 | 7772962 | 1951713 |
| 5 | ITR-4S | 1628312 | 2947568 | 846543 |
| 6 | ITR-5 | 765054 | 851327 | 144709 |
| 7 | ITR-6 | 593047 | 638184 | 14922 |
| 8 | ITR-7 | - | - | 2710 |
| Grand Total | | 16433684 | 21486807 | 10321775 |

**(E) Internet users in India**

Digital signature users are proportional to the internet users. The below Graph was taken from the **world development indicator**. By observing the below graph we see that not even 1% of the population of India used the internet. By 2007 it rose to around 4%. These percentages of

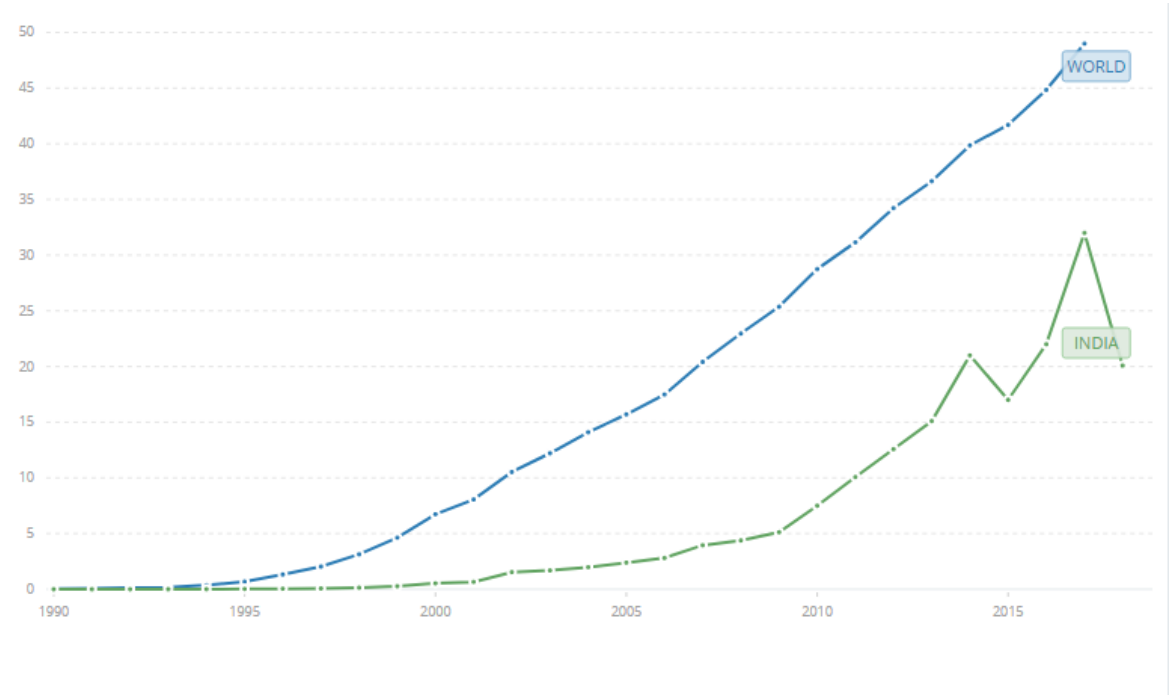
internet users kept on increasing and by 2015 17% of the population was using the internet which jumped to 24% in 2019.

But when comparing the internet usage of India it is pretty low keeping the fact in mind that India is one of the most populated countries in the world.

If we closely look in the below graph we will see there is a sharp decline in the internet usage from 2017 to 2018. In 2017 it was around 32% which came down to 21% in 2018. The same happened between 2014 and 2015.

The literacy rate has a significant impact. According to the 2011 Census of India, India's literacy rate was 74.04 percent. That indicates that 26% of the Indian population is unlikely to utilise the internet, which means that 26% of the Indian population is unlikely to use digital signatures. There are others as well.In India, there are 422.8 million persons under the age of 18. ( Census of India). As a result, 1.5 percent of the population of India, who is above 18 years old and literate, uses Digital Signature.

**Individuals using the Internet (% of population) (1990-2019)**




## V. COMPARISON BETWEEN DIGITAL SIGNATURE IN SWEDEN AND INDIA

Around the same time, both countries were exposed to the concept of digital signature. However, there are differences in awareness and usage for the following reasons.

Almost everyone in Sweden has access to the internet (International Telecommunications Union (Geneva), June 2013).[11] And students use digital signatures to acquire their

scholarship money and loans from the government, and tax forms are filled out using digital signatures, making digital signatures a common practise in Sweden. There are 6 million people who utilise digital signatures that is around more than 60% of the population of Sweden uses it.

In India, digital signatures are mostly utilised to file tax returns. And not everyone uses a digital signature to file their tax return; it is only required to use a digital signature for tax filing if the company's annual revenue exceeds 10 million rupees or if the annual turnover of an individual exceeds 10 million rupees. An individual's annual income exceeds 2.5 million rupees. The Controller of Certifying Authorities, India, has only issued roughly 5.2 million digital signatures since 2000, which is a considerable number, but only 0.43 percent of the Indian population uses digital signatures.

In Sweden, banks offer digital signature certificates, but in India, government appointed corporations distribute them. This has a significant impact on awareness.

Because digital signature certificates are issued by banks and have the validated information of their customers upfront, the procedure of granting DS is simple. It's also available to download on the bank's websites.

In India, only a few certifying authorities, the listed organisations that have been assigned by the CCA, issue digital signatures. Furthermore, the person must be physically present with an identification card in order to obtain a digital signature.

As a result, the digital signature is not easily accessible to Indians, resulting in lower usage and awareness of the product.

## VI. IMPROVEMENTS TO INCREASE USAGE OF DIGITAL SIGNATURE

In Sweden, the public can easily obtain a digital signature through banks. Using internet banking, you can also download a digital signature certificate from the bank's website. Because the bank has verified customer information, it is simple for the bank to give digital signatures to its customers, making the process of obtaining a digital signature certificate quick and straightforward.

There are only seven certifying authorities in India where the public can obtain a digital signature. To obtain the digital signature certificate, the individual must be physically present in the CA office. It is not easy to get digital signatures for Indian citizens.

Thus, increasing the availability of DS in areas where people have more access, such as banks or post offices, can improve its usability in India.

 [ISSN 2581-5369]

## VII. FUTURE WORK

The developing country can follow the industrialised countries in using digital signatures in several industries, hence increasing product utilisation and, as a result, user numbers.

In India, the adoption of digital signatures might be boosted by making them available in public areas such as banks and post offices. The ease of access to digital signatures will also raise public knowledge of digital signatures.

Mobile phones and tablets should be able to use digital signatures, increasing the frequency with which they are used in India. Since 2010, Swedish banks have offered mobile bankID services.

Global organisations can choose digital signature certificate providers, which increases trust between two parties when e-trading takes place between countries. Almost every country's e-authentication law is based on the Model Law for E-Commerce established by the World Bank. UNCITRAL; establishing a standard international rule for the use of digital signatures will be simple.

Due to time constraints, the study is limited to two countries: one developing and one developed. The study needs to be carried out in other countries in order to collect more data and get a comprehensive picture of worldwide awareness of digital signatures.

*****

 [ISSN 2581-5369]

## VIII. REFERENCES


1. Saha Payel,(2016),*"A comprehensive study on digital signature for internet security"*
2. Thangavel Jayakumar,(2017),"*Digital Signature: Comparative study of its usage in developed and developing countries*".
3. R.L. Rivest, A. Shamir, and L. Adleman (1977): "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*.
4. Shafi Goldwasser, Silvio Micali And Ronald L. Rivest (1988): "*A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks."*
5. Sakib AN, Mahmud T, Mountain Munim S, Rahman MM.(2021)*"Secure authentication & key exchange technique for IEEE by using cryptographic properties"*,(pp. 43-47)
6. Kessler Gary C (1998),*"An Overview of Cryptography"*
7. Hartman B, Flinn DJ, Beznosov K, Kawamoto S.(2003) "Mastering web services security. John Wiley & Sons"
8. Alidoost Nia Mehran, Sajedi Ali ,Jamshidpey Aryo (2014),"*An Introduction to Digital Signature Schemes"*
9. Schoaba Vagne, Gomes Felipe,Branco Castelo Luiz (2011): *"Digital Signature for Mobile Devices: A New Implementation and Evaluation. International Journal of Future Generation Communication and Networking"*
10. Singh Deeksha , (2018)*,"Critical Analysis of Digital Signature Laws in India"*
11. Kalaluka L, (2020), *" The electronic communication and transaction bill 2020"*
12. Pordesch U, Berger A. (1999) *"Context-sensitive verification of the validity of digital signatures. Multilateral Security for Global Communication."*
13. Kain K, Smith SW, Asokan R.(2002) *"Digital signatures and electronic documents: a cautionary tale. In advanced communications and multimedia security"* (pp.293-307)
14. Jøsang A, Al Fayyadh B. Robust WYSIWYS (2008) *"a method for ensuring that what you see is what you sign. In proceedings of the sixth australasian conference on information security*" (pp. 53-8).
15. Haber S, Stornetta WS.(1990) *"How to time-stamp a digital document. In conference on the theory and application of cryptography"* (pp. 437-55).


*****