IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

Digital Signature in ITR Filing

Kesiya Johnson[1], Dr. Sarika S[2]
Student of MSC, Department of Computer Science, Naipunnya College, Thrissur, India[1]
Assistant Professor, Department of Computer Science, Naipunnya College, Thrissur, India[2]

Abstract: *Everyday new technologies are brought and progressed very rapid in all fields. Now new generation gifted totax payers for filing their income tax go back via on-line is E- submitting. The E-filing is the new effective method of filing income tax return through online and make E-payment tax with digital signature. It saves our golden time, strength, fee and also reduces our anxiety. So, the tax payers are required to use E- filing centres. This present look at examines that the existing customers are satisfied with the E-filing facilities but most of thepeople tax payers are not aware to the E-submitting proceduresso sufficient steps are required for create greater awareness within the minds of tax payers regarding submitting of earnings tax with the aid of using digital signature.*

Keywords: Taxpayers, E-filing, Digital Signature, Tax, etc.

I. INTRODUCTION

The advanced technology is seen everywhere, from e - ticking to e-filing the tax return, everything can be done easily at the comfort of your home. While filing an income tax return online a requirement that you have to furnish is to affix your digital signature with yourtax return documents to authenticate these docs. In the IT Act 2000,a digital signature enjoys the identical status as a normal signature.It attests and verifies that the taxpayer has authenticated the tax return documents in secure surroundings, without fraud. Virtual or Digital signatures, that are issued by Certification authorities, contain particulars just like the taxpayer's name, public key, name of issuing Certification Authority, expiration date of public key(12years), the digital signature and its serial wide variety. Tampering with digitally signed files and claiming forgery over digital signatures isn't a viable option, especially since some assessments are nearing completion to confirm the same. Changes and additions to digitally signed files are also included in the signingprocess.

II. CRYPTOGRAPHY

Cryptography is a method of defensive facts and communications through the usage of codes, so that only those for whom the information is intended can read and process it. In computer science,cryptography refers to comfy data and conversation techniques derived from mathematical concepts and a fixed of rule-based calculations called algorithms, to transform messages in ways which might be difficult to decipher. these deterministic algorithms are used for cryptographic key technology, digital signing, verification to defend data privateness, web surfing at the internet and private communications which includes credit card transactions and email.

A. Objectives of Cryptography

1. Confidentiality: The information cannot be understood by anyonefor whom it was accidental.
2. Integrity: The statistics can't be altered in storage or transit between sender and supposed receiver without the alteration being detected.
3. Non-repudiation: The creator/sender of the information cannotdeny at a later degree their intentions in the advent or transmission of the facts.
4. Authentication: The sender and receiver can affirm every other'sidentity and the starting place/vacation spot of the statistics.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

B. Types of Cryptography

1. Symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the sender uses to encrypt data (encryption) and the receiver uses to decrypt it(decryption). This only required a single key for both encryption and decryption process. Block and Stream algorithms comprise symmetric key cryptography, which is widely used on the Internet today. Two popular encryption algorithms are the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES). This method of encryption is often faster than symmetric encryption, but it allows both the sender and the data receiver to have access to the secret key.
2. Asymmetric key algorithms: It use a pair of keys, a public key associated with the sender for encrypting messages and a private key that only the receiver knows for decrypting that information. This required two key one to encryption and the other one to decryption. When someone wants to send an encrypted message, they will retrieve the recipient's public key from a shared directory and use it to encrypt the message until it is sent. The receiver will next use their associated private key to decrypt the message. When the sender encrypts a message with their private key, the message can only be decrypted with the sender's public key, allowing the sender to be authenticated. These encryption and decryption operations are fully automated, so users do not have to manually lock and unlock messages.

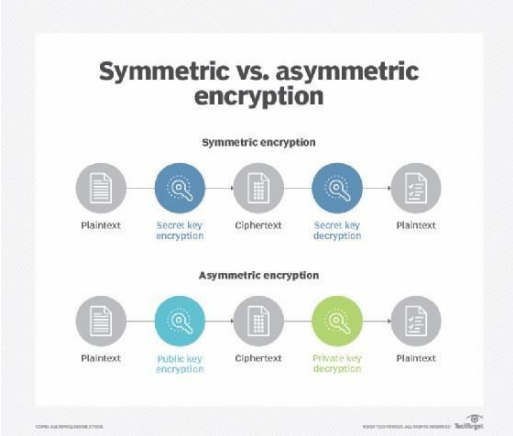

Figure 1: Types of Cryptography

III. DIGITAL SIGNATURE

A mathematical algorithm is routinely used to validate the authenticity and integrity of a message using a digital signature, which is a type of electronic signature (e.g., an email, a credit card transaction, or a digital document). Digital signatures are used to identify users and protect information in digital messages and documents by creating a virtual fingerprint that is unique to them. The email content becomes part of the digital signature in emails. Electronic signatures such as digital signatures are far more secure than other types of electronic signatures. Digital signatures can offer proof of origin, identity and standing of digital files, transactions or digital messages. Signers also can use them to renowned knowledgeable consent. In many countries, including the United States, digital signatures are considered legally binding inside the identical manner as conventional handwritten record signatures.

A. How DSC Works

Digital signatures are based on asymmetric key cryptography or public key cryptography. Using a public key algorithm, such as RSA algorithm, two keys are generated, creating a linked pair of keys, one private key and one public key. Digital signatures work through asymmetric key cryptography's two mutually authenticating cryptographic keys.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

The individual who creates the DS uses a private key to encrypt signature-related data, the only way to decrypt that data is with the signer's public key. If the recipient cannot open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated or valid.

Figure 2: DSC Verification

B. Different Classes of Digital Signature

Class 1 Certificate: These are issued to individuals or private users. This Certificate confirms that the user's name and e- mail ID are valid and approved by the Certifying Authorities on their database.

Class 2 Certificate: These are issued only to business personnel and individuals. They confirmed that the information in the application provided by the subscriber is the same as the information in popular consumer databases.

Class 3 Certificate: These are issued only to individuals and organizations. They are very high assurance certificates, mainly for the purpose of e-commerce applications. It is issued when the individual appears in-person before the certifying authorities.

C. Benefits of Digital Signature

1. A digital signature can't be edited or tampered with.
2. It is secure to track a digitally signed document.
3. It brings down the wastage of paper and is an eco- friendly.
4. Helps the efficiency of the entire e-filing process.
5. Reduces cost

Table 1: DSC Comparison

	Digital Signature
Visible	No
Unobtrusive	Yes
File changes	Not Allowed
Virtually attached to file	Yes
Physically embedded infile	No
Data authenticity	Yes
Copyright protection	Yes
Global identification	partial

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

D. Certifying Authorities for Digital Signature

The licensed certifying authorities who authorized by governmentappointed Controller of Certifying Authority:

1. Safe scrypt
2. Capricorn CA
3. IDRBT
4. GNFC
5. eMudra CA
6. NSDL e-Gov CA
7. Indian Air Force
8. Verasys CA
9. CDAC CA

E. How to Get Digital Signature

The purpose of obtaining a digital certificate, the user will have to submit certain documents to the certifying authority (CA). It includes an application form that has been duly signed, a passportsize photo an identification proof, Aadhaar card number, PAN card verification etc. The applicant may be asked to provide the mobile number, email address and home or organization address of the user. The different countries will have different requirements from the applicants for the issuance of digital signature certificate. The process of obtaining digital signature certificates varies depending on the certifying authorities.

F. Mandatory Taxpayers for ITR Filing using DSC

Digital signature certificates are mandatory for some services / usercategories such as e-Verification of returns filed by politicalparties and companies as well as other persons whose accounts are required to be audited under Section 44AB of the Income TaxAct. In other case, it is optional.

G. Steps to create DSC in ITR filing

1. Fill up the Income Tax Return form, generate the file as anXML (Extensible Mark-up Language) file and save it.
2. Step in to the Income Tax India website. Log in to your accountusing your user password and ID.
3. After login, click on the tab "Submit Return" and then select theassessment year.
4. Select the Income Tax Return Form Name from the drop-downmenu list.
5. The next field will be "Do You Want to Digitally Sign the File?"Then select the "Yes" button.
6. Select the type of digital signature you want to use, it can be "Sign with USB Token" or "Sign With .PFX file".
7. Upload the ITR with the help of digital signature certificate andverify it.

Figure 3: USB Token

H. Current Problem in Taking DSC

As previously stated, the signature is signed with the USB token after the digital signature certificate has been verified and approved by certified authorities. The password will be included in the DSc. There's a chance you'll

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

lose your USB token. If it is lost, other people or hackers can quickly track down the clients DSc by targeting all of their authentication information. This is a fairly rare problem in this field.

IV. PROPOSED SYSTEM

The problem mentioned above is an example of a threat. We can use an OTP password with the USB token to get around this situation. If someone tried to access the USB Token, they could easily access the password that has been attached to it. It may also request an OTP verification in addition to the password. Only the client's mobile number will receive the OTP password. As a result, this will provide a security mechanism which useful in future attacks.

V. CONCLUSION

From the above study, the usage of ITR filing using DSC must be focused to make a better way of using online method in a developing country like India. Still the usage of DSC is increasing day by day among the citizens for its secure techniques. This study focuses on the digital signature and its authentication process. The basic objective of research is to provide an awareness about DSC and its basic attacks. The majority of individuals are unaware of this problem. The paper aids them in raising awareness about the problem. This case study will be implemented in my future research.

REFERENCES

[1] B. A. Fourazan, Debdeep Mukhopadhyay, "Cryptography and Network Security", Tata McGraw Hill, 2nd edition, pp.15,210234,2010Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2020.
[2] Alqad, Ziad, et al. "A New Approach for Data Cryptography." International Journal of Computer Science and Mobile Computing 8.9 (2019): 30-48.
[3] Curry, Ian. "An Introduction to Cryptography and Digital Signatures." Entrust Securing Digital Identities and Information (2001).
[4] Aysu, Aydin, Bilgiday Yuce, and Patrick Schaumont. "The future of real-time security: Latency-optimized lattice-based digital signatures." ACM Transactions on Embedded Computing Systems (TECS) 14.3 (2015): 1-18.
[5] Alfred M., Oorschot P., and Vanstone S., Handbook of Applied Cryptography, CRC press, 1997