ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Securing SAP Invoices using Document Signer Certificates

[1]Mrs. K.E. Eswari, M.C.A., M.Phil.,M.E., Associate Professor/MCA,
[2]Ms. S. Priyadharshini, III MCA.,
Department of MCA, Nandha Engineering College (Autonomous), Erode-52.
Email ID: eswari.eswaramoorthy@nandhaengg.org, priyadharshinip20@gmail.com

Abstract*—With the development of Internet, digital signature becomes more and more important for the electronic documents security because of its data integrity protection and privacy. Almost every reasonable scale organisation needs to issue invoices and many more documents. For medium to large businesses, there are substantial benefits in eliminating paper and the associated handling and postage costs. Typically core financial data is held electronically and invoices are archived in digital form to avoid the costs and retrieval issues when using paper-based archiving. Online information systems allow organisations to improve their efficiency, substantially reduce their costs, enhance their green credentials and comply with regulatory requirements. Having timely and reliable access to accurate, final, approved and archived information is today's business imperative. The present paper focuses on a comparative study of existing algorithms of digital signature on the basis of many hard problems.

***Index terms:*Digital signature, Digital Sign, Non-repudiation, Integrity, SAP**

I. INTRODUCTION

In the current scenario, a variety of data transfer is made possible across the internet using various methods. From these data some of the information is highly secret which requires a great security, thus, an extensive security measures have to be adopted. Many algorithms and techniques can be used to secure our data or information from threats. These kinds of technologies and algorithms are collectively known as Cryptography.

Cryptography system can be widely categorized into two parts first one is symmetric key cryptography (single key system) which is possessed by both the sender and receiver and another one is public key system (asymmetric key cryptography) in which uses of two keys are provided, first is public key which is common for both the sender and receiver and other one is private key which is known to the individual only.The ability of safeguarding information by modifying it (encoding it) into a non-readable pattern is termed as cipher text. Also, those who acquire a private key, can decode (or decrypt) the information into the plain text. Various techniques are included under the cryptography to provide security, digital signature is one of them.

II. DIGITAL SIGNATURE

Basically, Digital signatures are based on asymmetric key cryptography.Digital Signature is primarily a mathematical application of asymmetric cryptographic method over the digitized documents to certify its legitimacy and integrity to its users. Digital signature can be used to provide assertion that the claimed party authorized the information.

In addition to this, it can be used to identify whether or not the information was altered after it was signed (i.e., to detect the reliability of the signed information).A Digital signaturealgorithm consists key generation, Signature generation, Signature Verification algorithm. A Digital Signature should provide Authentication, Integrity and Non-repudiation.

A. Regulatory requirements

With any digital document it is easy to create realistic but fraudulent documents. Unprotected electronic documents make it extremely hard for recipients to determine if the document is genuine, who the originator is, whether they are authorised to release it or whether it has been modified since its creation. Within Europe the EU VAT Directive aims to prevent VAT fraud by mitigating such risks. The Directive requires that: "Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed". The only standard and interoperable way of doing this is to use digital signatures and in general EU member states require that a qualified electronic signature is used to confirm the identity of the originator. EDI systems can be used however VAT authorities can still insist on paper summaries being provided for EDI. The Directive also requires that "The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period".

B.Digital Signatures And Business Benefits

The most effective way of meeting these requirements is to use industry standard digital signatures. These bind the identity of the sender with the data content in a way that clearly shows if the document has changed. Digital signatures deliver trust services that are effective both immediately and for many years of archive storage. Authenticity and integrity are assured, and the time of approval is also bound into the document. The use of PDF/A (ISO 19005) format documents guarantees that everyone can display and print the document both now and for many years to come.

Digital signatures provide an effective way of mapping wet-ink paper signatures to the electronic world. The protection offered by the cryptographic processes is extremely robust and uses multiple international standards for widespread interoperability. Without this form of protection important business data is open to abuse, manipulation, fraud, denial and theft.

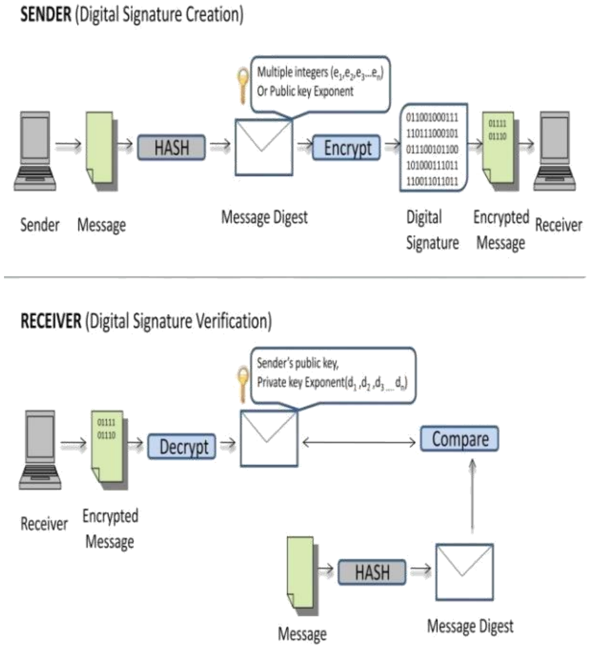

Figure 1. Digital Signature Process

A digitally signed invoice enables a recipient:

- To confirm who sent the invoice, when they signed it and their current trust status (by checking and validating the signers digital certificate)
- To confirm the document has not been changed either now or later, be it weeks, months or even years (by verifying the digital signature)
- To confirm the originator meant to send it – it is not a draft unsigned document andthat the originator cannot deny approving and sending it (by verifying the signature)
- To save time and substantial monthly costs in invoice printing, paper, postage andarchive/storage (by enabling paperless workflows)
- To meet the needs of the EU VAT Directive and where required using QualifiedElectronic Signatures to ensure signature acceptability within

C. Non-repudiation

At the sender side, the data encoded using the private key of the sender may only be decoded with the interrelated public key. Sender sign a message with the private key of himself/herself and the public key of the sender is used to authenticate the validity of the signature. To authenticate the transmitting data generated from both sides; the sender cannot deny that the signature is sent by him/her.

As shown in the above figure, the sender sends a message encrypted by his/her own private key and creates a signature and send it to the receiver. By using sender's public key at the receiver side message is decrypted and it verifies the signature and retrieves the original message being send by the sender.

III.APPROACHES

Digital Signature Algorithm (DSA) is the part of Digital Signature Standard (DSS) approach, which is developed by the U.S. National Security Agency (NSA).DSA is a Federal Information Processing Standard for digital signatures. in August 1991 DSA is developed by the National Institute of Standards and Technology (NIST).There are two different approaches to the Digital Signature:

A.RSA Approach

In this approach, RSA, named for Ronald Rivest, Adi Shamir, andLeonard Adleman, the developers of the algorithm, isthe best known of all the public key algorithms.The key feature of RSA is that it is a reversiblealgorithm. (Technically, RSA, or any public keyalgorithm, is not reversible. Public key algorithms areone-way functions.

We say RSA is reversiblebecause the data that was transformed with one keycan be recovered with a different key.) With RSA, wecan use a private key to recover the data that waspreviously encrypted using the public key. Thepublic key is used to encrypt data. The private key isused to decrypt the data. Since the public key isavailable to anyone, but only the owner of the keypair has the private key, anyone can encrypt datameant for the key's owner and only the key's owner can decrypt the data.

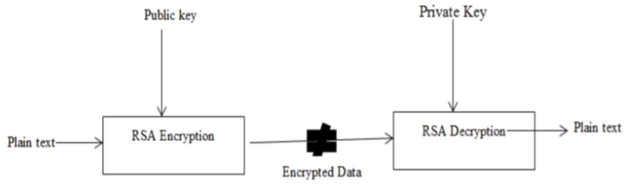

Figure 2: RSA Encryption and Decryption

1. Firstly, a message digest is being calculated.
2.Then to sign the digest of the message, a privatekey is used.
3. Before transmitting it to the recipient, the signatureis appended to the message.
4. The digest of the received message is then beingcalculated by the recipient.
5. After that, verifying of the signature will requireextracting of the signature from the message andusing RSA on the signature with the public key.
6. If in case, the result of the transformation and thenewly calculated digest is equal, the signature isvalid

Sending the Signature: -

Taking (m, Y) where m is message, Y is signature.
$Y=m^d.(\text{mod}n)$

Where (n, e, m, Y) are publicly declared, and (p, g, d)are privately declared, (p, and g) are large primenumbers,

n = modulas = p.g,
e = public exponent,
d= private exponent (secret key) = e^{-1}. (modQ(n)), and
Q(n) = (p-1) (g-1).

Verifying the Signature: -

$Y = m^{d.e}$. (mod n)

Where, we must know from prior that, d.e=1;

Hence,
$m^{d.e}= m$.

If signature is valid, we have to check, whether,

$Y^e= m$.(mod n)

B. MD5 Approach

MD5 algorithm was developed by Professor RonaldL. Rivest in 1991. In this algorithm, a message ofarbitrary length is taken as an input and producesoutput as a 128-bit “fingerprint” or “message digest”of the input. The MD5 algorithm is intended fordigital signature applications, where before beingencrypted with a private (secret) key under a publickeycryptosystem such as RSA, a large file must be compressed in a secure manner.

The exact same RSA algorithm used for encryptioncan be used for digital signatures. Using RSA for a signature is

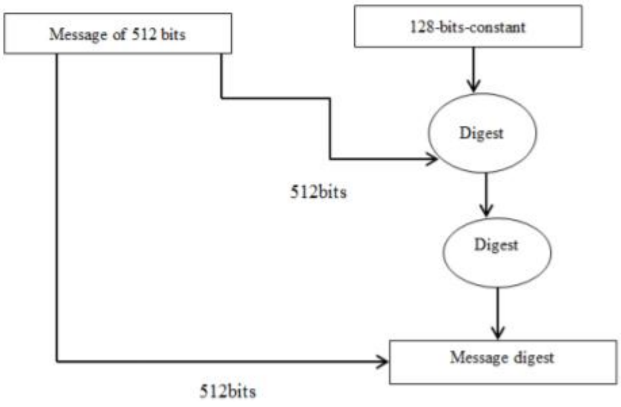

Figure 3: MD5 Algorithm

Suppose there is a Sender A and a Receiver B Senderend: -

If A wants to send a message to B.

- Sender A input hash function, it generates randomnumber of keys to a signature.
- Signature is formed with the help of private keyencryption.
- Signature + Original message is send to theReceiver B.

Receiver end: -

When B receives the message from A.

Signature is decrypted with public key

When the received message from the decryption ismatched with the original message and results to besame, we cansay that the message has properlyreceived from source to destination without losing itscontents and provides all internet securityrequirements i.e. integrity, confidentiality,nonrepudiation, and authentication etc.

C. DSS approach

This approach makes usage of a hash code function. In the signature function hash code is given just as an input, additionally a random number is also produced on this specific signature. In the signature function, sender’s private key (Pr) and set of constraints (we can say that this set is used to invent a global public key (PUG)) which are also called as batch of broadcasting principals plays a vital role. From this result is generated which is a signature comprising of two components s and r. Hash code value is generated at the receiver side for the entering messages. After that hash code value with the signature is transferred for the signature verification. In the phase of signature verification, verification function is depending on the sender’s public key (Pu) paired with private key on the global public key. From the verification function, resultant value isgenerated which is same as the signature component r, this shows that the signature is legitimate.

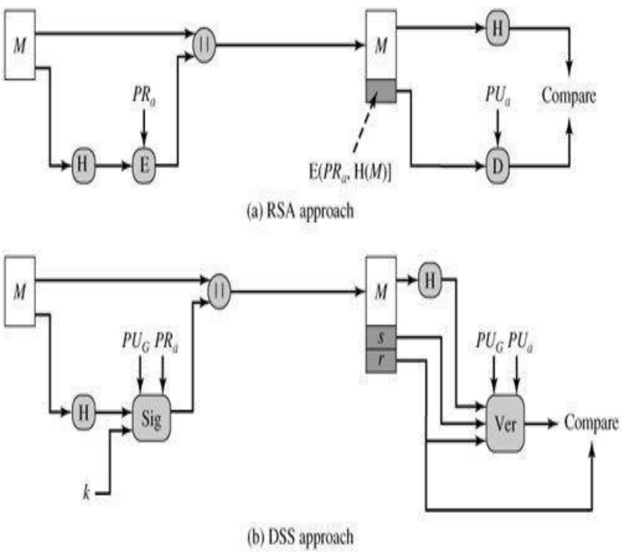

Figure4: Approaches

IV. PROPERTIES

Properties of Digital Signature can be described as follows for which it has been chosen in Internet and Digital Security: -

- The signature must be an authentic one that means the recipient should understand that the signer signed the document.
- It must not be unalterable, i.e. the electronic document should not be changed once it is signed by someone.
- Signature should be non-repudiatable, which means after the signer signs a document then the signer cannot claim that he has not signed.

V.REVIEW ON VARIOUS DIGITAL SIGNATUREALGORITHMS

Some of the Digital Signature algorithms based on above approaches are discusses below:

Daniel Julius Bernstein proposed a “Edwards-curve Digital Signature Algorithm (EdDSA)” is a digital signature algorithm using a variant of Schnorr signature based on Twisted Edwards curves. It designs a fastest digital signature schemes without compromising security. Like other discrete-logarithm based signature schemes, EdDSA uses a secret value called a nonce unique to each signature. After generating a private key, there is no requirement of a random number generator for EdDSA. There is no risk of a broken random number which will be involved in revealing the private key in the digital signature process.

Kamal kr Agarwal proposed a” digital signature algorithm based on Xth root problem”. In this paper, he introduced a new theoretic problem based on hard number. This theoretic problem based on hard number can be used in the field of cryptography which is a new variant of algorithms of digital signature on the basis of the problems of elucidating the Xth root problem. The paper also depicts a summarizing study of the Xth root problem & the eth root problem. In this, a single signature is used for verification. The functioning of the projected algorithm that are based on multiple hard problems are found to be competitive to the majority of the algorithms based on digital signature.

Ashish Vijay proposed a “A New Variant of RSA Digital Signature”. In this paper, he introduced a new alternative of the different algorithms of digital signature that are based on two hard problems, the Xth root problem & the problem of prime factorization. The presented algorithm in this paper is an alteration of the original RSA based digital signature algorithm. In this algorithm, two signatures are used for verification. This algorithm is secure against various attacks while it is insecure against the Chosen-message attack like RSADSA

Kapil Madhur proposed a “Modified ElGamal over RSA Digital Signature Algorithm (MERDSA) “This paper is based on two hard problems, prime factorization (FAC) and discrete logarithm (DL). In this algorithm two signatures is used for verification. The proposed algorithm carries out the security analysis and performance. In this paper, we have reviewed that when an oracle 'O' splits Prime Factorization & DiscreteLogarithm then it can split the presented algorithm, if the public key of the scheme and a message madv is provided.SushilaVishnoi proposed a” A new Digital Signature Algorithm based on Factorization and Discrete Logarithmproblem” this paper also focuses on two multiple hard problems, the Discrete logarithm & the problem of prime factorization. Time complexity of the proposed algorithm is also calculated. In this algorithm a single signature is used for verification.

VI. CONCLUSION

In this paper, review on different algorithm of the Digital Signature which is based on RSA and DSA approach has been implemented using SAP invoices. A digital signature is computed using a set of rules and a set of parameters such that the identity of thesignatory and integrity of the data can be verified.New variation of algorithms of digital signature that are based on multiple hard problems like the elliptic curve, discrete logarithm and prime factorization has also been discussed.

It comes from the information safety and the valid protection to privacy, so information safety and privacy protection are most important problems forSAP or any financial documents. The main aim of the text is to apply digital signaturetechnology in SAP financial documents, advance the solution tothe safety problems of digital signature technology in and offer identity certification to those whotake part in business activities, which prevents all kinds of potential safety hazards. The study and application of digital signature technology in India has a disparity with international level. Based on the comparative analysis, we showed the performances based on many characteristics.

REFERENCES

[1] ES Ismail, NMF Tahat, and RR Ahmad. A New Digital Signature Scheme Based on Factoring and Discrete Logarithms. Journal of Mathematics and Statistics.

[2] D. Boneh and H. Shacham. Fast variants of RSA. CryptoBytes (RSA Laboratories)

[3] Ashish Vijay, Priyanka Trikha, Kapil Madhur, "A New Variant of RSA Digital Signature".

[4] Kapil Madhur, Jitendra Singh Yadav,Ashish Vijay, "Modified ElGamal over RSA Digital Signature Algorithm (MERDSA)"

[5] Kamalkumar Agrawal, Ruchi Patira, Kapil Madhur," A Digital Signature Algorithm based on Xth Root Problem"

[6] Bernstein, Daniel J.; Duif, Niels; Lange, Tanja; Schwabe, Peter;Bo-YinYang (2012). "High-speed high-security signatures".

[7] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. Information Theory, IEEE Transactions on, 31(4):469{472, 2002}