Digital signature verification with Etoken based Authentication in local area network

[1]Ms.P.Abinaya , [2]M.Mariselvi,[3] M.Veeralakshmi, [4]A.Shanthi, [5]M.Nandhinishree,
[1]AP , Department of CSE ,Ramco Institute of Technology, Rajapalayam,.Tamil Nadu, India
[2]Department of CSE ,Ramco Institute of Technology, Rajapalayam,.Tamil Nadu, India

Abstract— *In this paper, we are proposing the automatic generation of digital signatures by using the newly developed digital signature algorithm BS-PDSS(Probabilistic Digital Signature Scheme) in the templates like Microsoft Word, Excel and PowerPoint with the additional security as the E-Token based authentication. This BS-PDSS algorithm will make use of two dissimilar crypto-graphic assumptions as Integer Factorization (IF) and Discrete Logarithm (DL). Nowadays security is the more important in areas like army and navy and other defence applications. So we are proposing this project for highly secure local area networks like Army, Navy and other defense application. Although there are more file formats are used, Microsoft products are most often used one. So we are proposing this concept on Microsoft products like word, Excel, and PowerPoint. Within that local area network, the creator and the reader of the document must be authenticated, using the highly secure authentication. Although they are using the secure authentication, there is no automatic generation of the digital signature, whenever they are creating any document. So we are proposing the automatic generation of the digital signature in the above products.Although there is an option for explicitly signing the documents, nobody is using that nowadays. So we must have the constraint that, everybody must sign their documents with their digital certificates while creating the document itself. So we are using the authentication for both the creator and the reader of the document so that no other can read the documents except the authenticated users. Although we have system login-based authentication, If the user leaves the system as it is after login, then anybody can use your system for making any malfunction. So we are proposing this "E-Token based two-factor authentication". This will prompt the user to authenticate for two times. One is whenever they are using the system. Next whenever they are trying to create a new document.*

Keywords——.*Digital Signature, Integer Factorization Problem, Discrete Logarithm problem, Forgery, Etoken, PDSS*

I. INTRODUCTION

Now a day's security is the more important in areas like army and navy and other defence applications. Although there are more file formats are used, Microsoft products are most often used one. So we are proposing this concept on Microsoft products like word, Excel and PowerPoint. Within that local area network, the creator and the reader of the document must be authenticated, using the highly secure authentication. Although they are using the secure authentication, there is no automatic generation of digital signature, whenever they are creating any document. So we are proposing the automatic generation of digital signature in the above products.Although there is a option for explicitly signing the documents, nobody is using that now-a-days. So we must have the constraint that everybody must sign their documents with their digital certificates, while creating the document itself.So we are using the authentication for both the creator and the reader of the document, so that no other can read the documents except the authenticated users. Although we have system login based authentication, If the user leaves the system as it is after logon, then anybody can use your system for making any malfunction. So we are proposing this "E-Token based two factor authentication". This will prompt the user to authenticate for two times. One is whenever they are using the system. Next whenever they are trying to create a new document.

II. GOAL

The main goal of our project is to secure the document which is present in the local area network by providing confidentiality, authentication, integrity Non-Repudiation and Availability have to be taken under the security head.

III. APPLICATION

A. Design and implementation

This digital signature generation solution is designed to work in a pluggable mode and can be made to work in any current/existing versions of MS Office. This means that the old versions are also supported the feature of automatic digital signature generation. Here we are using the existing secure digital signature generation algorithm known as PDSS algorithm. For embedding the digital signature algorithm into MS word and excel, we are using VBA(Visual Basic for Applications). Application has been designed to provide confidentiality, authentication, non repudiation and integrity. In Microsoft Office, they have used the RSA with SHA1, which has collision vulnerability. But BS-PDSS prevents the document from collision vulnerability and basic attacks.

B. RSA with SHA1

Word processor like Microsoft Word and Microsoft Excel, Microsoft PowerPoint uses SHA1 with RSA for digital signature generation, Where SHA1 is a hashing algorithm (Document and certification signing) while RSA is an encryption/decryption algorithm (Secure communications).To start with, It is certainly not a bad idea to avoid SHA-1 when other algorithms exist, which do not have the SHA-1 weaknesses to anyone's knowledge

C. Our analysis on RSA with SHA1

The security of SHA-1 depends on how the user's using it. The vulnerability is what's known as a *collision vulnerability*: an attacker has the ability to create two input strings with the same SHA-1 hash with less computational power than it should take him for a good hash function. However, he does *not* get to freely pick what either of those input strings is, and he does *not* necessarily have the ability to feasibly find a string whose hash matches that of any particular string. If the attacker has *any* control over *anything* you are willing to sign, collision attacks *might* be exploitable. In 1978, Ron Rivest, Adi Shamir and Leonard Adleman (RSA) designed first widely accepted encryption and signature scheme using IF problem. This application has the property of deterministic that would get same cipher text or digital signature for same message at every time. The security of signature scheme is based on hardness of the IF problem along with intractability of RSA problem (extraction of e th root problem). The RSA signature scheme has two kind of applications; message recovery as well as in appendix. In appendix type of application, it is existentially as well as selective forgeable and also suffers with basic attacks due to multiplicative property.So this paper conclude that these schemes are forgeable. Therefore, two very popular digital signature schemes using DL and IF problem have been proposed which is BS-PDSS Scheme.The computational complexity (asymptotic running time) of IF and DL problems depends on integer multiplications.

D. **BS-PDSS scheme**

This section presents a new "BS-PDSS" using IF and DP problems. Next, two large k-bit (security parameter) primes $p = 2p` + 1$, $q = 2q`+ 1$ (Sophie-Germian primes) are selected and composite modulus is computed as $N = pq$.
Then, an element $g \in Z * N$ (generator of the group $Z * N$) is selected of having order $\lambda(N`) = p`q`$.

After computing $(g, N, \lambda(N`))$, an algorithm for BSPDSS is proposed, which is as follows.

1.Algorithm: BS-PDSS

1. After computing $(g, N, \lambda(N`))$ on given security parameter k, a number $X \in Z\lambda(N`)$ is selected randomly and public exponent $Y = g^{X} \bmod N$ is computed. The public and secret exponents pairs are (N, Y, g) and $(N, X, g, \lambda(N`))$ respectively.

2. In signature signing algorithm, a integer $k \in Z\lambda(N`)$ is selected randomly and computed a signature pair$(\sigma1, \sigma2)$ for message M by using secret exponent $(N, X, g, \lambda(N`))$ such that $\sigma1 = g^{k} \bmod N$ and $\sigma2 = k^{-1} (M - X) \bmod \lambda(N`)$.

3. The signature pair , $\sigma1 = g^{k} \bmod N$, $\sigma2 = k^{-1} (M - X) \bmod \lambda(N`)$ is verified by using public exponent (N,Y,g) of signer for input message M by computing $V1 = g^{M} \bmod N$, $V2 = (Y \sigma_1^{\sigma2}) \bmod N$. Then, by checking $V1 == V2$, Itis decided that if yes then accept, reject otherwise.

Analysis for the BS-PDSS

This section presents that how the use of these two problems; IF and DL problems together makes secure from forgery as well as from basic attacks without the use of OWCH function.

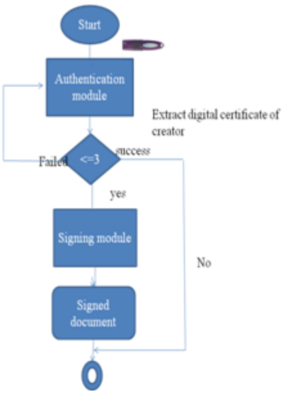


Figure 1 Flow chart of Signing module

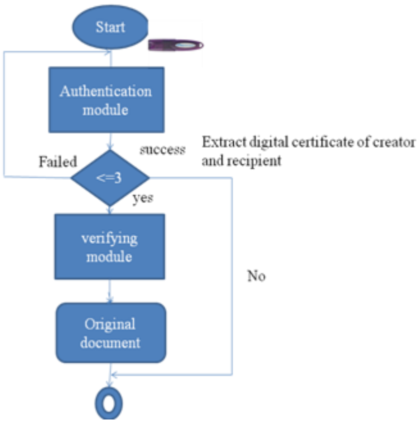
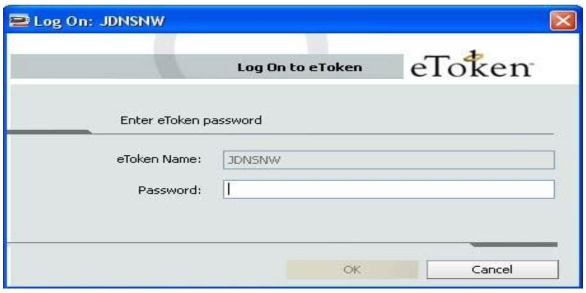


Figure 2Flow chart of Verification module

E. *Etoken based Authenication*

Issue of Authentication is resolved by the security device called Etoken.Etokens have the private key corresponding to the individual user. The E-token are USB based devices and use Crypto standard. PKI operations usually require certificates, private and public keys. Private keys are always securely stored on the E-token. Certificates are stored on E-token as this enables mobility .EToken enables setting token policies, performing basic token management functions. In addition ,E-Token provides users and administrators with a quick and easy way to transfer digital certificates and keys. E-Token Properties include an initialization feature allowing administrators to initialize tokens according to specific organizational requirements or security modes,and a password quality feature which sets parameters to calculate an E-token password quality rating.

An E-token is not to be removed from the USB port during an operation. Many operations, such as Authentication, certificate selection and signing the documents etc. require multiple actions. If the token is removed during one of these actions,the data structure on the token may need to be reinitialized .Public key certificate of the recipient(s) have to be present in the client machine,properly installed as well. The private key residing in the E-token cannot be retrieved by ordinary means by inserting in the USB port.It is programmed and after proper authentication mechanism it is used .CA certificates are downloaded on to an E-token.When the Etoken is inserted into the computer,one or more of these CA certificates may not be on the computer. In such a case ,the CA certificateis loaded on to the computer .When Single Logon mode is enabled, users can access multiple applications or multiple documents with only one request for the E-token password during each computer session.This all eviates the need to log on to each application separately.


Log On: JDNSNW

Log On to eToken

eToken

Enter eToken password

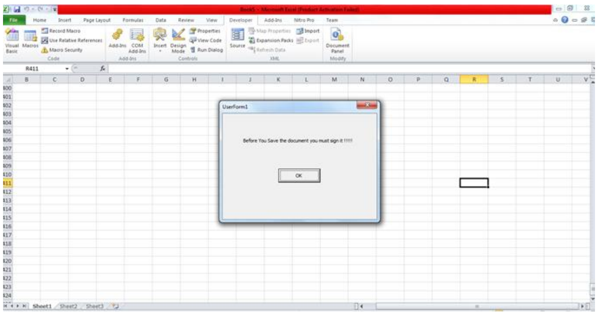
eToken Name: JDNSNW

Password:

Figure 3 E-token Authentication screen

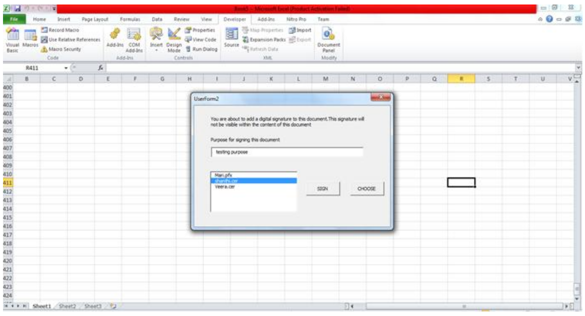
F. *Implementation*

1. *Signature generation in MS Excel:*


UserForm1

Before You Save the document you must sign it !!!!!

Figure 4.1 After saving the Excel document

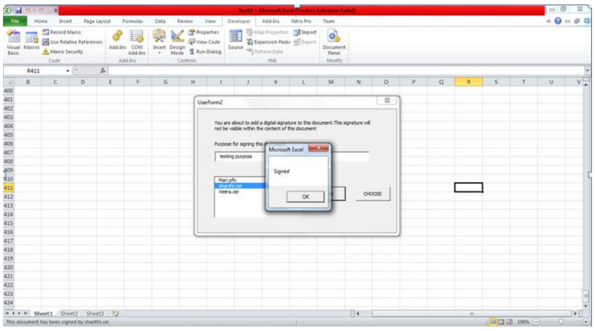

UserForm2

You are about to add a digital signature to this document.This signature will not be visible within the content of this document

Purpose for signing this document: testing purpose

Mari.pfx
shanthi.cer
Veera.cer

Figure4.2 Listing of the Certificates


UserForm2

You are about to add a digital signature to this document.This signature will not be visible within the content of this document

Purpose for signing this document: testing purpose

Mari.pfx
shanthi.cer
Veera.cer

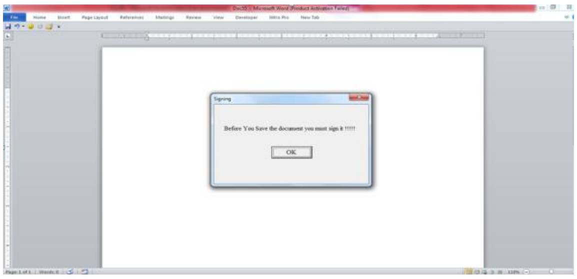
Microsoft Excel

Signed

Figure4.3 After Signing the Document

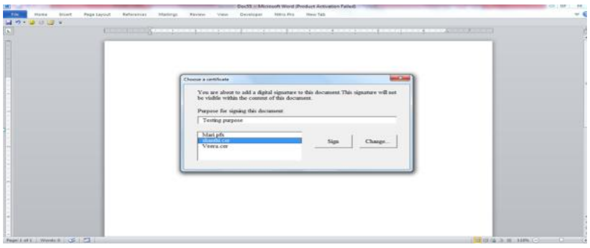
a.

1. *signature gerenation in MS Word*



Before You Save the document you must sign it !!!!!

Figure 5.1 After saving the Word document



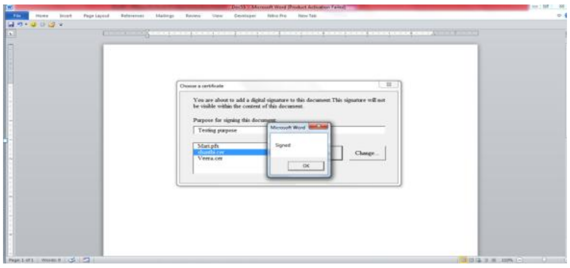
You are about to add a digital signature to this document.This signature will not be visible within the content of this document.

Purpose for signing this document

Testing purpose

Mari.pfx
shantha.cer
Veera.cer

Figure5.2 Listing of the Certificates



You are about to add a digital signature to this document.This signature will not be visible within the content of this document.

Purpose for signing this document

Testing purpose

Mari.pfx
shantha.cer
Veera.cer

Signed

Figure5.3 After Signing the Document

IV.CONCLUSION

This paper presents a new security feature of adding additional security to the secure local area network, which secure the documents from unauthorized access and other forgeries. This will provides the standard security for all the documents which is present in the local area network

Reference

1. Shailendra Kumar Tripathi and Bhupendra Gupta, "*An Efficient Digital Signature Scheme by using Integer Factorization and Discrete Logarithm Problem*" 978-1-5090-6367-3/17/$31.00 ©2017 IEEE
2. Rakesh Shukla, Hari Om Prakash, R.PhaniBhushan, *Signature with Two Factor Authentication"* 978-1-5090-5769-6/16/$31.00 ©2016 IEEE
3. RakeshShukla, Hari Om Prakash, R.PhaniBhushan, *Signature with Two Factor Authentication"*978-1-5090-5769-6/16/$31.00 ©2016 IEEE
4. *S.*Goldwasser, S. Micali, and R. L. Rivest, "*A digital signature scheme secure against adaptive chosen-message attacks*," SIAM Journal on Computing, vol.17,no.2,pp.281–308,198
5. P. Kumar and B. P. Dungdung, "*An extension of elgamaldigital signature algorithm*," Ph.D. dissertation, 2012.
6. D.Bleichenbacher,"*Generating eigamal signatures withoutknowing the secret key*," in Advances in Cryptology—EuroCrypt'96.Springer, pp. 10–18, 1996.
7. S.R.Subramaniya, B.K.Yi ,"*Digital Signatures*" 10.1109/MP.2006.1649003 of 2008