ISSN 2395-1621

Implementation of Digital Signature over the Intra-net

[#1]Swarup Bam, [#2]Akshay Chavan, [#3]Nilesh Nandawadekar,
[#4]Prof W. P. Rahane

[1]swarupbam@gmail.com,
[2]akiichavan@gmail.com,
[3]lilstarnilesh@gmail.com,
[4]wasudeo.rahane@sinhgad.edu

[#1234]Department of Information Technology,

NBNSSOE, Pune.

ABSTRACT

Distribution of digital document through insecure channel leads numerous questions of the integrity and the ownership of the document on the receiver's side. Employing digital signature algorithms solves the issues related to the receiver's proof and approval of the document from the sender along with monitoring the document if they have been altered by illegitimate parties. With the advancement in the electronic media usage, security of data is one of the major problems that we face. Moreover, signing of documents in traditional method is a tedious process. Digital signature helps in with all the above given. Signing of the documents with proper authentication can be done. The process of identifying the source of document can be simplified. This paper covers the various algorithms and methodologies needed for proper execution of the system.

KEYWORDS: Public Key Infrastructure (PKI), Certifying Authority (CA), Digital Signature Algorithm (DSA), Public Key (PU), Private Key (PR), One time Password (OTP).

ARTICLE INFO

Article History

Received: 27th April 2017

Received in revised form :

27th April 2017

Accepted: 29th April 2017

Published online :

4th May 2017

I. INTRODUCTION

Digital Signatures have been in legal use since last 10 years in many if the countries. There has been a major development in the use of Digital Signature since then. Digital Signature nowadays is an integral part of the any technology. Digital Signature is process of embedding data to a particular document that determines its authenticity and the ownership of the document. Digital Signature can be applied in various forms i.e documents, images, sound etc. This paper solely focuses on the application of Digital Signature on documents using various algorithms. [2]These schemes of using Digital Signature can be classified as visible and invisible. Scheme using visible watermark for owner protection [3][4][5][6][11] and that using invisible watermark scheme [7][8][9][10]. Signing of documents traditionally is quite a tedious process. There are various problems like security, forgery and storage of the documents as it occupies lot of physical space. This is where Digital Signature helps i.e. signs the document along with providing in depth dimensional security. The area of concentration in this project is establishment of Public Key Infrastructure (PKI). PKI is the basic component of the system. Key generation, key distribution, providing security and authentication are the basic functionalities in the system. Key generation process generates two keys i.e. public key and private key. Private Key is used for encryption the message and public key for decryption of the message. Figure 1 shows the general way in which a document is signed digitally. We will be using PDF documents of the signing purpose.[3] The general structure of the PDF document consists of header, body, cross-reference table and trailer. The security is increased with the help of an OTP method used to verify the users. The OTP is sent through the Certifying Authority to the sender before he/she signs and sends the PDF.

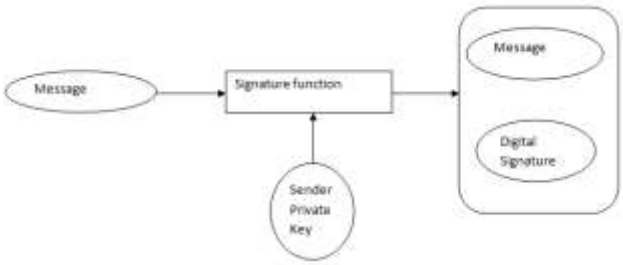

Figure 1

The important facet in this is the establishment of Public Key Infrastructure (PKI). The PKI will consist of a Certifying Authority (CA) and the users. Digital Signature has been explained in part III. PKI is explained in IV part. The algorithm used i.e DSA is explained in part V and respectively. The proposed system s is mention in part VI.

II. MOTIVATION

Now a day's everything is becoming digital, traditional method of signing the documents has some limitations. Digital signature can overcome these limitations by providing security and authentication. Most of traditional systems are been now replaced with a digital systems. The project is an improvement over the existing traditional approach of signing of documents physically. The proposed system will speed up the process of signing documents. The storage of physical paper is also a tedious process along with a risk that the document might be completely destroyed.

III. DIGITAL SIGNATURE

The Digital Signature notion is similar to that of a physical signature. It involves the use of keys i.e public keys and private keys for signing and verification of document along with the algorithm it uses. Let us consider the following assumptions for the better understanding of the process of Digital Signature:-

a) Let DC denote the Digital document to be signed in this it is a PDF.

b) Let PU and PR be the Public and Private keys respectively.

c) Let SG be the signature associated with the document.

The function (SG=Sign (PR, DC) on the sender side is responsible of signing the PDF, which uses the senders private key PR and the document DC for signing. The receiver reverses this process in which it uses the senders public key PU and the document DC for verification purpose i.e if the document is been sent be the anticipated sender. As the PU is given it must be computationally infeasible to determine PR for any attacker. [2] On the other hand, given PU and a set of signed documents X = (DC1, DC2….., DCn) together with a set of the signatures produced from all the element in X, Y = (SG1, SG2,⋯. SGn) an attacker must not be able to determine a valid signature on any document DC where DC ≠ X.

Signing of large size documents can consume a lot of computational power. This problem here is solved by using the hash function that produces a fixed length hash value for the documents. This can be given as (SG=Sign (H(D),PR)), where H is the hash function.

The receiver has to verify that the hash value computed matches with that of the digitally signed documents; this entire process is done by the verification function on the receiver side. In this paper we will be using the DSA as our algorithms for digitally signing of the PDF.

IV. PUBLIC KEY INFRASTRUCTURE

PKI is the structure which is very important in implementing this method of digital signature. It consists of an administrator and users in that network in this case it is the intra-net network.

As there will be use of PU and PR, there must a central authority. Key generation, key distribution, providing security and authentication are the basic functionalities of PKI.

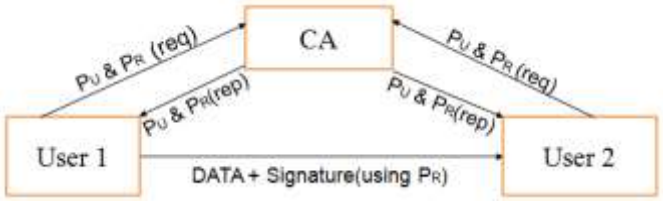

Figure 2

In the key generation process two keys are generated i.e public key (PU) and private key (PR). Private Key is used for the signing of the PDF, while Public Key is used for the verification purpose. The administrator or the Certifying Authority (CA) is responsible provides a pair to each to the users. Administrator has the right to revoke the keys provided to the users. As verification of documents is done through the CA it is important to protect this against the attackers, but as being on an intra-net network the risk factor is reduced moreover there is a login procedure to be followed if one manages to enter the intra-net.

V. DSA

DIGITAL SIGNATURE ALGORITHM:

[14]The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

i) Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS. The hash output may be truncated to the size of a key pair.

ii) Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1,024 (inclusive). NIST 800-57 recommends lengths of 2,048 (or 3,072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N. FIPS 186-3 specifies L and N length pairs of (1,024, 160), (2,048, 224), (2,048, 256), and (3,072, 256). N must be less than or equal to the output length of the hash H.

iii) Choose an N-bit prime q.

iv) Choose an L-bit prime modulus p such that p − 1 is a multiple of q. Choose g, a number whose multiplicative order modulo p is q.

v) This may be done by setting $g = h(p-1)/q \bmod p$ for some arbitrary h ($1 < h < p - 1$), and trying again with a different h if the result comes out as 1. Most choices of h will lead to a usable g; commonly h = 2 is used. The

algorithm parameters (p, q, g) may be shared between different users of the system.

Signing of the document is done as follows:

Let H be the hashing function and m the message:

1) Generate a random pre-message value
2) Calculate r= (gk mod p) mod q.
3) In the unlikely case that r=0, start with a different random k.
4) Calculate s= k-1 (H (m) +xr) mod q.
5) If s=0 then start again with a different k.
6) The signature is (r, s).

Verifying the key:

1) Reject the signature if 0<r<q or0<s<q is not satisfied.
2) Calculate w= s-1 mod q.
3) Calculate u1=H (m). w mod q.
4) Calculate u2=r. w mod q.
5) Calculate v= (gu1yu2 mod p) mod 1.
6) If v=r the signature is valid.

VI. PROPOSED SYSYTEM

The system which we have created is quite the simple one. There is a Public Key Infrastructure establishment containing the Certifying Authority along with the users. The users can both new and existing. The overall system works around the signing of PDF documents. This is a take over the traditional approach of signing of documents. All the constraints mentioned above are been used in this system. A brief view of how the system works at the Sender, Receiver and Certifying Authority.

Signing of document (sender):

1. Verify credentials.
2. Request for PR and PU.
3. Sign the PDF.
4. Receives an OTP and enters it.
5. Sends the PDF.

Verifying the document (receiver):

1. Verify credentials.
2. Authenticate the PDF.
3. Read the contents.

Certifying Authority:

1. Verify the credentials.
2. Provide with PR and PU.
3. Provide OTP.

Brief overview about the system:

The user logins into the system using his/her credentials which are verified by the CA. The user requests for private key and public key. Private Key as the name suggest is only known to the user while the Public Key might be known to everyone present in the system as the communication i.e sending the documents is done with the help of the receivers Public Key. On receiving the pair of keys from the Certifying Authority the sender gets ready to send the required document in this case a PDF. The sender uploads the document and enters the name of the intended user, the system asks for a OTP which is sent to the sender by the CA as he/she wants to send it. Upon the successful verification of the OTP by CA the document is ready to be sent. Sender signs and sends the document to the intended user. The Signing of PDF is using the Private Key out of the pair provided to the CA to the sender. The receiver gets an alert mail for the received document. Receiver verifies his/her credentials. The receiver checks if he was the intended receiver or not if yes then the Public Key and Private Key is match else not a match and the document is available or absent according to the verification.

Thus the system is completely used for digital signing of the documents, speeding up the process in turn.

REFRENCES

1) Self-Contained Digitally Signed Documents Approaching "What You See Is What You Sign" Håkan Söderström Söderström Programvaruverkstad AB Stockholm, Sweden hs-at-soderstrom.se.

2) Protection of Integrity and Ownership of PDF Documents using Invisible Signature Imad Fakhri Al Shaikhli_, Akram M. Zekiy, Rusydi H. Makarim_, Al-Sakib Khan Pathan_Department of Computer Science,Department of Information System Faculty of Information and Communication Technology, International Islamic University Malaysia Gombak, Selangor, Malaysia imadf@iium.edu.my. 978-0-7695-4682-7/12 $26.00 © 2012 IEEE DOI 10.1109/UKSim.2012.81

3) B.-B. Huang and S.-X. Tang, "A contrast-sensitive visible watermarking scheme," Multimedia, IEEE, vol. 13, no. 2, pp. 60 – 66, april-june 2006.

4)Y. Hu and S. Kwong, "An image fusion based visible watermarking algorithm," in Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on, vol. 3, may 2003, pp. III–794 – III–797 vol.3.

5) S.-K. Yip, O. Au, C.-W. Ho, and H.-M. Wong, "Lossless visible watermarking," in Multimedia and Expo, 2006 IEEE International Conference on, july 2006, pp. 853 –856.

6) S. Mohanty, R. Sheth, A. Pinto, and M. Chandy, "Cryptmark: A novel secure invisible watermarking technique for color images," in Consumer Electronics, 2007. ISCE 2007. IEEE International Symposium on, june 2007, pp. 1 –6.

7) S. Bandyopadhyay, D. Bhattacharyya, and P. Das, "Hybrid digital-embedding using invisible watermarking," in Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference on, june 2008, pp. 1881 –1885.

8) M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in Image Processing, 1997.Proceedings., International Conference on, vol. 2, oct 1997,pp. 680 –683 vol.2.

9) A. Huggett and C. Stubbings, "Invisible watermarking for digital video applications and challenges," in Secure Images and Image Authentication (Ref. No. 2000/039), IEE Seminar on, 2000, pp. 9/1 –9/6.

10) T.-Y. Chen, D.-J. Wang, T.-H. Chen, and Y.-L. Lin, "A compression-resistant invisible watermarking scheme for h.264," in Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09. Fifth International Conference on, sept. 2009, pp. 17 –20.

11) M. Kankanhalli, Rajmohan, and K. Ramakrishnan, "Adaptive visible watermarking of images," in Multimedia Computing and Systems, 1999. IEEE International Conference on, vol. 1, jul 1999, pp. 568 –573 vol.1.

12) Digital Image Authentication and Encryption using Digital Signature,Shahzad Alam,Amin Jamil,Ankur Saldi,MusheerAhmed,Department of Computer Engineeringand Technology, Jamia Millia Islamia, NewDelhi, shahzad5alam@gmail.com , 978-1-4673-6911-4/15/31.00 © 2015 IEEE.

13) Electronic flow document in the university environment using public-key infrastructure. Radek Holý1, Marek Kalika1, Lukáš Vopařil21Computing and Information Centre,2Faculty of Transportation Sciences, Czech Technical University in Prague, Czech Republic radek.holy@cvut.cz, marek.kalika@cvut.cz, lukas.voparil@cvut.cz

14) On the Security of Two Pairing-Based Signature Schemes Rouzbeh Behnia, Syh-Yuan Tan and Swee-Huay Heng Facurity of Information Science and Technology Multimedia Univerisy Melaka, Malaysia Email: rouzbeh.behnia, sytan, shheng@mmu.edu.my 978-1-4673-6537- 6/15/$31.00 ©2015 IEEE.

15) Agent-based PKI for Distributed Control System Sergi Blanch-Torn´eEscola Polit`ecnica Superior sblanch@alumnes.udl.cat Fernando Cores Distributed Computing Research group fcores@diei.udl.cat Universitat de Lleida. Spain Ramiro Moreno Chiral Cryptography & Graphs Research group ramiro@matematica.udl.cat 978-1-908320-58/2/$31.00 ©2015 IEEE.

