Generation and Verification of Digital Signature with Two Factor Authentication

Narayan Ranjan Chakraborty
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
narayan@daffodilvarsity.edu.bd

Muhammad Taifur Rahman
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
taifurrahman929@gmail.com

Md. Ekhlasur Rahman
Computer Science and Engineering
Daffodil International University
Dhaka, Bangladesh
ekhlasurrahman07@gmail.com

Mohammad Shorif Uddin
Computer Science and Engineering
Jahangirnagar University
Savar, Bangladesh
shorifuddin@juniv.edu

***Abstract*—This paper is intended to provide a cloud-based digital signature platform with biometric authentication and establishes an enhanced security solution in the field of cryptography. We proposed a new schema of digital signature where signature generation and verification is done on the cloud environment. Like Public Key Infrastructure each user owned a pair of key – private key and public key. A signer has to confirm his biometric identification (vein pattern) and a one-time key verification to access the private key for signing a document. This one-time key (OTK) is only shared between the signer and the receiver additionally they use it for a single document signing or verification. Before the verification of a signature or a document, a receiver also needs to prove his identity using his vein pattern. To complete the verification process, he/she must provide the public key of the signer and the shared one-time key to the system. Thus our system gives a confidential interaction between the signer and the receiver of the document.**

***Keywords*—Cryptography; Digital Signature; Finger Vein; MD5; One-time Password.**

I. INTRODUCTION

In today's world e-commerce, e-government, e-business is omitting their conventional documents into e-document. But information tempering, signature forgery of alteration has been increasing remarkably. As a result, from business organization to the ordinary user who signs a document digitally can be a victim of digital crime. To assure the security of digital signature, most widely accepted scheme is Public Key Infrastructure (PKI) which is relied on two pair of keys: private key and public key[8]. Although PKI is widely accepted method, it has some drawbacks. [14] A public key algorithm (e.g. RSA) is used to produce this pair of keys [15]. Frauds target this private key of clients or Certificate Authority (CA) to pretend as a signer and using this key can easily sign the documents. So the main concern of the PKI based security system is to protect the keys. Generally, private keys are stored on a device using a password or PIN which can be guessed easily. Another approach to protect private keys is to store them on a smart card which needs to be purchased from a trusted source and needed to be carried with for signing. If for any reason the cardholder loses his card then he could end up facing some unexpected issues. Somehow someone else gets that card and wishes to use the private key of a signer and signs a message, then it is impossible to detect that the signer is not the actual cardholder and he did not sign the message. Furthermore, CA may use old keys to issue new certificates for the clients [7].

II. LITERATURE REVIEW

Xiaodong Liu, Quan Miao and Daxing Li [1], presented A New Special Identity Based Signature Scheme where a signer needs to provide his/her fingerprint in the Key Generation Center (KGC) during registration. After that finger print is converted into a public key string and issued a corresponding private key by the KGC. To claim this private key, it is mandatory for a signer to confirm his identification using his fingerprint. During the verification, receiver used the public key (came from the singer) to reconstruct the fingerprint. After that the singer is recommended to provide his finger print on the spot to match with the reconstructed finger print. Although this system identifies the signer using his biometric, the signer is forced to the verification process.

Ahmed B. Elmadani [2], proposed a system that generates unique keys (Ks, Kr) for the singer and the receiver from their extracted face image to digitally sign a message. Both unique keys are combined together to encrypt and decrypt the calculated fingerprint of the document. Singer sends the fingerprint of the document (which is already encrypted by combined key, Ksr), the document itself and his Signing Key. These three parameters are encrypted with the receiver's key. Finally, the receiver uses his/her key to decrypt the received

978-1-5090-5769-6/16/$31.00 ©2016 IEEE

encrypted message and generates a new fingerprint of the document to match with the previously received document fingerprint although the system gives an error rate 1.65. Hitachi, Ltd [3], Developed a secure digital signature technology where finger vein is used as a secret key instead of using a smart card or a password for user authentication. The scheme is strong as the Water Signature claimed by Hitachi Ltd.

Sambangi Eswara Rao and S. Ravi Kumar [4], used iris as a biometric and proposed a solution to generate private key from the biometric template (512 byte iris code template) and used one-way hash function to provide protection of the biometric template. This Paper presented two systems using RSA and DSA. Additionally, they suggested not to transmit the biometric template over the internet for authentication and eliminated the key management issues of PKI by avoiding the private key storage. Finally, authors also discussed the problem about the correctness of all bits of the template. A.M. Al-Khouri and J. Bal [5], suggested to use three-factor authentication for digital identification. Authors described a trio technology that integrated PKI with smart card and biometrics for precise identification. The Main advantage of this proposal is that nobody can use the smart card but the cardholder.

Wojciech Kinastowski [6], proposed a protocol for data exchange and message signing in the cloud environment. According to the protocol public and private key pair is stored on the cloud where the private key is encrypted with a password that is only known to the signer. To access this private key a one-time password is generated using a hardware security module (HSM) and send it to the signer's cell phone. The protocol provides an excellent usability (eliminate dedicated devices like smart card, card reader etc.) and cross platform requirement in the cloud communication, however it does not provide sufficient verification to detect the precise identification of the signer. If the Singer lost his cell then anyone can access the private key using his OTP.

III. Proposed System

A. System Architecture

In our proposed system, signature generation and verification process are done in the cloud platform. As all we know in PKI, each user has a pair of keys: private key and public key. Private keys are stored on a central secure server. Our main target is the protection of this private key and provide a maximum possible security level, to achieve this goal we will use a hardware security module (HSM) to the application server.

To access this private key and sign a document signer has to face two-factor authentication i.e. something you are - Biometric identification and something you have – One-Time Key (OTK) - a randomly generated code. So the system allows a user to sign if his biometric vein image template is matched with the previously stored template in the database and it generates a key (OTK) then send it to the signer's mobile. After that the signer returns it back to the application server to complete the signature operation. This key is used for a single session only and known between the signer and the receiver to provide confidential interaction between them. The scenario of signature generation is represented in fig. 1

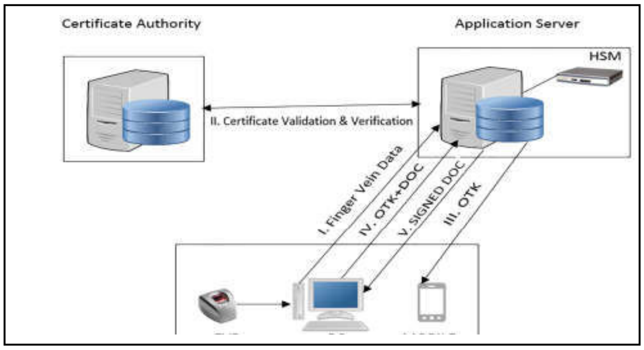


Fig. 1 Generation of Digital Signature

Signer sends his finger vein data using a vein reader to make an authentication request to the application server from the user terminal. The server manages the user's certificates and validates them with the help of the certificate authority. The server returns the signed document to the user when the signature process is done.

During signature verification, receiver also needs to provide his vein data to prove his authenticity. This time receiver just provides the OTK and public key to the server to complete the verification process. Then server displays the verification information of the document to the receiver. This story is exposed in fig. 2

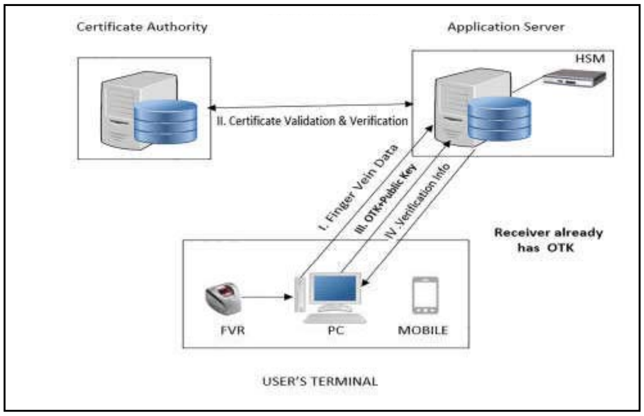


Fig. 2 Verification of Digital Signature

Forum of European Supervisory Authorities has been considered positively the concept of implementing digital signature remotely or the server-side. [16] Additionally, some trusted provider like Ascertia and DocuSign has been introduced cloud based digital signature system which is performed in the server-side environment and authorize the user with SMS-tokens. [17], [18]

B. System Algorithm

In this section we will discuss about the functions and algorithms which is used in the system. One time key: We have used *random_int* function which use Mersenne Twister's algorithm that generate cryptographically secure pseudo random integer.

```
function one_time_key($min,$max){
    $otk=random_int($min, $max);
    return $otk;
}
```

Public key: We have used md5 (which takes signed document contents) algorithm which is also encrypted by using modified base64 algorithm that makes documents more secure than before.

```
function generate_public_key($document_content){
      $unique_random_string=md5($document_content);
      $base64_string=base64_encode($unique_random_string);
     $modified_$base64_string=str_replace( ' + ' , ' . ',
                                                   $base64_string);
     $public_key = substr($modified_base64_string,0, $length);
     return $public_key;
}
```

C. Biometric Selection

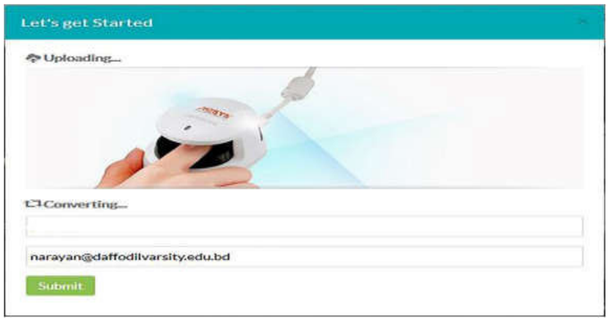
PKI does not identify the actual signer. If we use biometric instead of PKI, it removes dedicated devices and identify the actual signer. [1] Authors suggest to use some biometric like fingerprint, face, hand geometry, voice, iris and retina to verify the signer's identity. We choose vein pattern as a biometric, it overcomes the various frauds associated with other biometric. [9], [10], [11] Finger vein biometric authentication technology detects an individual using the pattern of vein inside of a finger. Its false acceptance rate is one in a million, false reject rate is 1:10,000 and failure rate is extremely low. [12], [13] Vein pattern is usually blood vessels which carry blood, so the only live human body is workable to the authentication process. There is deoxyhemoglobin in our blood which consumes infrared lights, vein pattern then looks like black/dark outlines. With the help of infrared lights and a special camera image of vein pattern is captured. This image is transformed into the template and compared with the saved template during the authentication. We let this job to the vein reader such as Hitachi M2SYS reader, just put your finger and get authenticated."

IV. User Panel Implementation

To complete the signing and the verification process user must go through some system predefined procedures which are much easier than the existing system. We illustrated those procedures below:

A. Sign Up

To complete the registration process user needs to use his finger vein data only. Now the question is how system will collect the remaining information. We are assuming there is a public database maintained by the government contains the basic information (user name, address etc) about their citizens. This prevents the fake information of any user who will use our system. So the system will try to find his data in the database and if any match found, it will collect his information and save in the system. Finally as shown in fig. 3 user have to provide his current email address to complete the registration.



narayan@daffodilvarsity.edu.bd

Fig. 3 User signup

B. Login

During login into the system user needs to provide his vein data only which is easier than providing password or PIN. If the vein data match with our system database, then the system will allow user to sign or verify the document.

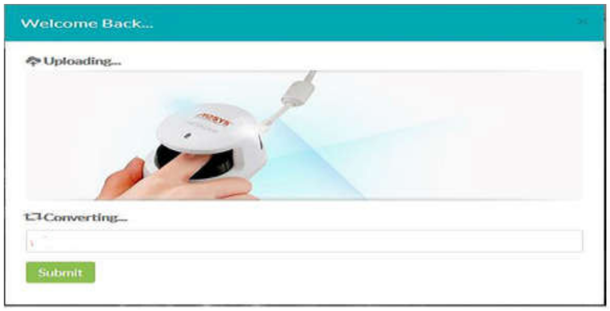
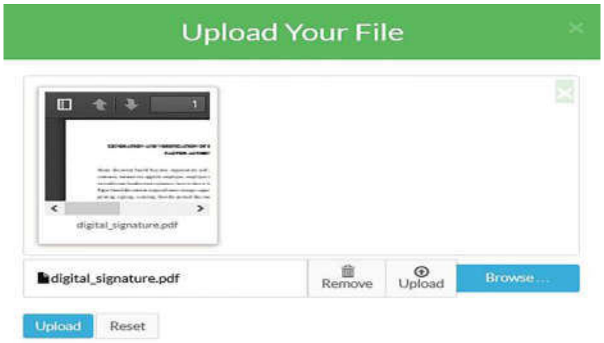


Fig. 4 User login

C. User authentication and document signing

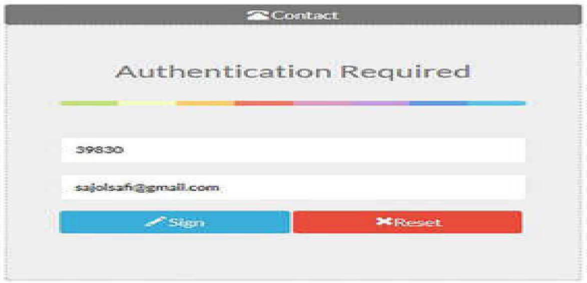
Before sign a document user uploads it to the system. Scenario is exposed in fig. 5.



digital_signature.pdf

Fig. 5 File upload page

When the signer is intended to sign a document the system will generate a One-Time Key (OTK) and send it to his email. Using an authentication form system ask the OTK from the signer as a proof of authenticity. From fig. 6 it is shown that signer specifies the email address of the receiver where he will get the same OTK.

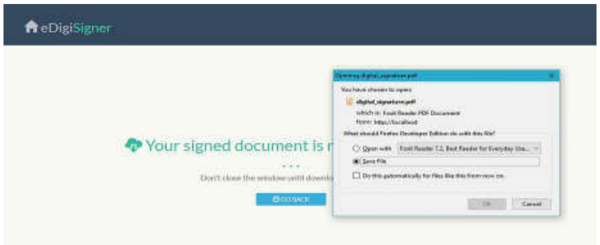


39830

sajolsafi@gmail.com

Fig. 6 User authentication

Thus the OTK is only shared between the sender and the receiver and system will provide a confidential interaction. Finally during signature generation, send a copy of OTK to the receiver's cell phone (e-mail) for document verification. Finally signed document is returned to the signer using browser default download option for his further uses as displayed in fig 7.


eDigiSigner
Your signed document is r
Don't close the window until downlo
GO BACK
Opening digital_signature.pdf

You have chosen to open:

digital_signature.pdf

which is: Foxit Reader PDF Document

from: http://localhost

What should Firefox Developer Edition do with this file?

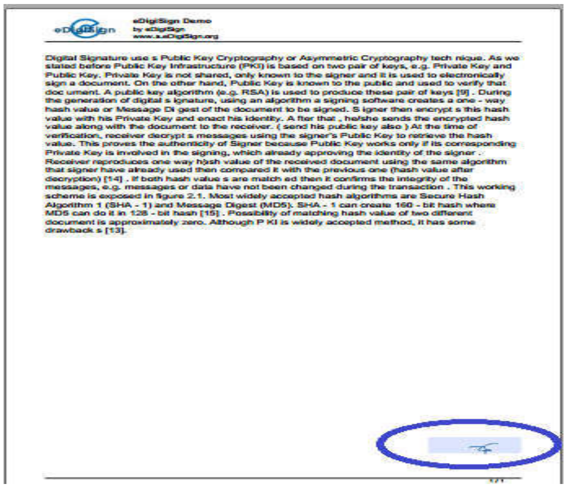
○ Open with Foxit Reader 7.2, Best Reader for Everyday Use...

● Save File

□ Do this automatically for files like this from now on.

Fig. 7 Downloading signed document

After downloading we will get the signed document as displayed in fig. 8. Signature is drawn on the right corner of the bottom of the document. User can click on the signature to see the signature properties.



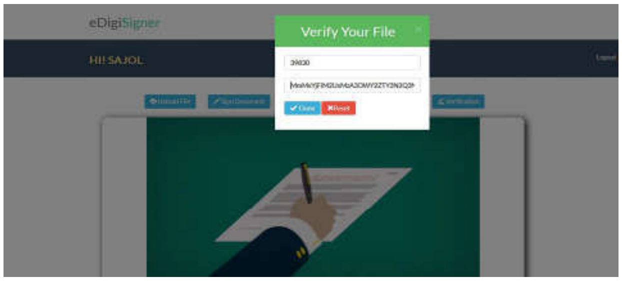
eDigiSign Demo
by eDigiSign
www.a.eDigiSign.org

Digital Signature use s Public Key Cryptography or Asymmetric Cryptography tech nique. As we stated before Public Key Infrastructure (PKI) is based on two pair of keys, e.g. Private Key and Public Key. Private Key is not shared, only known to the signer and it is used to electronically sign a document. On the other hand, Public Key is known to the public and used to verify that doc ument. A public key algorithm (e.g. RSA) is used to produce these pair of keys [9] . During the generation of digital s ignature, using an algorithm a signing software creates a one - way hash value or Message Di gest of the document to be signed. S igner then encrypt s this hash value with his Private Key and enact his identity. A fter that , he/she sends the encrypted hash value along with the document to the receiver. (send his public key also) At the time of verification, receiver decrypt s messages using the signer's Public Key to retrieve the hash value. This proves the authenticity of Signer because Public Key works only if its corresponding Private Key is involved in the signing, which already approving the identity of the signer . Receiver reproduces one way hash value of the received document using the same algorithm that signer have already used then compared it with the previous one (hash value after decryption) [14] . If both hash value s are match ed then it confirms the integrity of the messages, e.g. messages or data have not been changed during the transaction . This working scheme is exposed in figure 2.1. Most widely accepted hash algorithms are Secure Hash Algorithm 1 (SHA - 1) and Message Digest (MD5). SHA - 1 can create 160 - bit hash where MD5 can do it in 128 - bit hash [15] . Possibility of matching hash value of two different document is approximately zero. Although P KI is widely accepted method, it has some drawback s [13].

Fig. 8 Signed document

D. Document verification procedure

During document verification, receiver login to the system. After that system will ask the shared OTK and the public key of the signer. As all we know public key is available to all but OTK is only known between sender and receiver. Fig. 9 shows the verification process where first field contains OTK and second one contains public key of the signer.

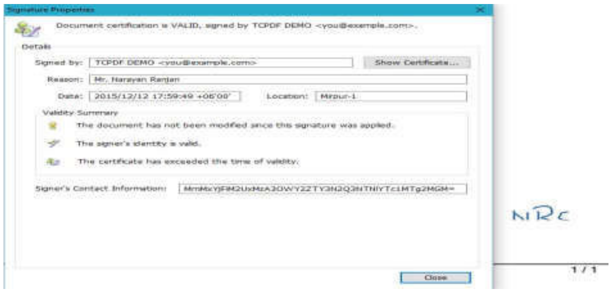


39830

MmMxYjFiM2UxMzA3OWY2ZTY3N2Q3

Fig. 9 Verification page

As displayed in fig. 10 receiver also may find the public key from the signature property of the signer.



Document certification is VALID, signed by TCPDF DEMO <you@example.com>.

Details

Signed by: TCPDF DEMO <you@example.com>

Reason: Mr. Narayan Ranjan

Date: 2015/12/12 17:59:49 +06'00'

Location: Mirpur-1

Validity Summary

The document has not been modified since this signature was applied.

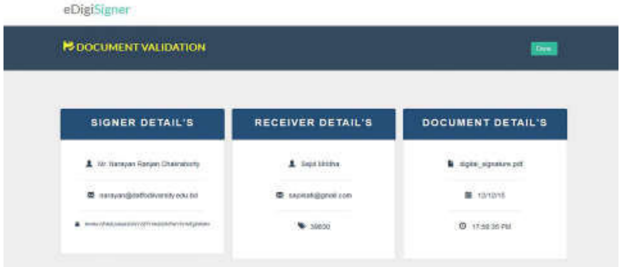
The signer's identity is valid.

The certificate has exceeded the time of validity.

Signer's Contact Information: MmMxYjFiM2UxMzA3OWY2ZTY3N2Q3NTNlYTc1MTg2MGM=

Fig. 10 Public key of signer

If provided information of OTK and public key is valid, the system will display the verification information about the document and the signer as shown in fig. 11.



SIGNER DETAIL'S	RECEIVER DETAIL'S	DOCUMENT DETAIL'S
Mr. Narayan Ranjan Chakraborty	Sajol Iktidha	digital_signature.pdf
narayan@daffodilvarsity.edu.bd	sajolsafi@gmail.com	12/12/15
[illegible]	39830	17:59:35 PM

Fig. 11 Document validation page

V. CONCLUSION

If a smartcard or a PIN is used to identify an individual then anyone can involve in signature generation or verification. Moreover there are a number of websites are still ongoing that provide fake ID including US, Canada and Bangladesh. Our main approach is to establish an improved digital signature scheme that satisfy the current business needs and fulfill the user satisfaction as well as obtain a scope for the future expansion within the organizational constraints.

Although biometric technology is quite expensive, it can provide increased level of security in the field of cryptography and digital signature.

VI. LIMITATIONS

Some restrictions of our system are listed below, 1) Since our system provides a cloud based digital signature platform, internet connection is required to adopt all of the services. 2) Required additional hardware such as a vein reader to detect vein pattern images. But this could be resolved if we could use smart phones to detect vein. 3) The Biometric vein technology is quite expensive.

VII. FUTURE WORK

Our system provides a confidential interaction between a signer and a receiver, only specified receiver can validate the document or message. If we send encrypted document to the receiver and share a Key (such as OTK) between them to decrypt the message then the data confidentiality also can be preserved. Additionally nowadays many mobile devices are coming up with the fingerprint image detection feature, in near future they will eventually meet the finger vein detection and our proposed system can be implemented with the mobile device integration.

REFERENCES

[1] Xiaodong Liu, Quan Miao and Daxing Li, “A New Special Biometric Identity Based Signature Scheme,” International Journal of Security and its Applications, vol. 2, no. 1, Jan. 2008.

[2] Ahmed B. Elmadani, “Trusted Document Signing based on use of biometric (Face) keys,” International Journal of Cyber-Security and Digital Forensics, vol. 4, no. 1, pp. 289-296, 2012.

[3] Successful development of biometric digital signature technology, available at http://www.hitachi.com/New/cnews/130218.html Last accessed on 15-07-2016 at 7:09pm

[4] Sambangi Eswara Rao and S.Ravi Kumar, “Novel Biometric Digital Signature System for Electronic Commerce Applications Using Java,” International Journal & Magazine of Engineering, Technology, Management and Research, vol. 1, no. 10, pp. 287-293, Oct. 2014.

[5] A.M. Al-Khouri and J. Bal, “Digital Identities and Promise of the Technology Trio: PKI, Smart Cards, and Biometrics,” Journal of Computer Science, vol. 3, no. 5, pp. 361-367, 2007.

[6] Wojciech Kinastowski, “Digital Signature as a Cloud-based Service,” The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013.

[7] AyshaAlbarqi, EtharAlzaid, Fatimah Al Ghamdi, SomayaAsiri and JayaprakashKar, “Public Key Infrastructure: A Survey,” Journal of Information Security, vol. 6, pp. 31-37, Jan. 2015.

[8] Rachana C.R., “The Role of Digital Signatures in Digital Information Management,” International Monthly Refereed Journal of Research in Management & Technology, vol. 2, pp. 103-109, Mar. 2013.

[9] Arulalan.V, Balamurugan.G and Premanand.V, “A Survey on Biometric Recognition Techniques,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, pp. 5708-5711, Feb. 2014.

[10] Rupinder Saini and NarinderRana, “Comparison of Various Biometric Methods,” International Journal of Advances in Science and Technology, vol. 2, pp. 24-30, Mar. 2014.

[11] Dr. Rajinder Singh and Shakti Kumar, “Comparison of Various Biometric Methods,” International Journal of Emerging Technologies in Computational and Applied Science, pp. 256-261, Feb. 2014.

[12] Learn about “Barclays brings finger vein biometrics to internet banking”, available at http://www.wired.co.uk/news/archive/2014-09/05/barclaysfinger-scanner. Last accessed on 17-07-2016 at 11:47pm.

[13] Learn about “M2-FingerVeinTM – Non-invasive finger vein reader” available at http://www.m2sys.com/finger-vein-reader/. Last accessed on 18-07-2016 at 03:00pm

[14] Carl Ellison and Bruce Schneier (2000), “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure,” Computer security journal, vol. xiv, pp. 1-8, 2000.

[15] Behrouz A. Forouzan, Data Communications and Networking, 4th ed., New York: McGraw-Hill, 2007.

[16] Forum of European Supervisory Authorities for Electronic Signatures (FESA), “Public Statement on Server Based Signature Services,” available at http://www.fesa.eu/publicdocuments/PublicStatementServerBasedSignatureServices-20051027.pdf.

[17] Learn about Cloud Signing - Multiple Signing in Options available at http://www.ascertia.com/Solutions/ByTechnology/cloud-signing

[18] Secure CoSign Digital Signature Use via One-Time-Password (OTP) Authentication available at http://www.arx.com/files/documents/cosigndigital-signatures-and-otp.pdf