ISSN:0975-9646

Implementation of PKI in Government Business

Shuchi Bhattacharya
Department of Computer Science and Applications
Dayananda Sagar College
Bangalore, India

Dr. Sumithra Devi K.A
Master of Computer Applications
R.V College of Engineering
Bangalore, India

Saurabh Bhattacharya
Managerial Consultant
Price Water House Coopers PWC Pvt. Ltd
Bangalore, India

Abstract— **This paper attempts to draft a strategy which can be adopted by Government bodies for migration of paper based communication to digital forms of communication. It utilizes the available existing technology and the legal framework created by IT Act 2000 and its subsequent amendment in the year 2008 for developing a suitable model which can be easily adopted by Government Businesses across the spectrum. It will try to cover all the aspects required to automate Government Financial Systems by developing an integrated financial management solution. It will trace a model which can be adopted for implementing principles of non-repudiation, data security & integrity in an electronic environment.**

Keywords-Authenticity, Confidentiality, Digital Signatures, Non-Repudiation, PKI

I. INTRODUCTION

The implementation of PKI in Government business, poses considerable challenges mostly to do with development of futuristic technical processes corresponding to the existing manual processes. One such challenge is to ensure that digital execution of processes are not hampered or slowed by manual interventions. E.g. if a process executed through a software requires physical signatures over a hardcopy printout for concluding the task then the entire advantage of having the process executed through a software will be lost. Thus migration of all paper based communication to electronic communication poses a challenge which ought to be solved for realizing entire potential of any Government Financial System. Such challenges can be overcome by unconventional solutions.

The IT Act 2000 was a major step for promoting the use of digital signatures. This Act enforced the Central Government to appoint a Controller of Certifying Authority. Later on the Root Certifying Authority of India (RCAI) was created as a root of trust in the hierarchical PKI architecture [1]. An amendment to IT Act in 2008 has introduced a new term E-Signatures to broaden the scope of the IT Act to include other techniques for signing E-Records as and when new technological concepts are available [2].

Though IT Acts have provided legal and technological framework for implementation of digital signatures, if any Government Financial System wants to shift from hardcopy based communication to softcopy based communication, in a way that all forms of communication which the department intends to do with other participating agencies such as Banks, Accountant General, etc. through hardcopy will be conducted through softcopy, requires architecture along with the support of technology. With the support of technology and statutory frameworks it is convenient to migrate such communications to softcopy form without diluting the necessity of non-repudiation and security.

This has been made possible because of two key technologies Encryption and Digital Signing. Encryption ensures data security and confidentiality, digital signing ensures non-repudiation. Going forward in this paper we will discuss mechanism which any financial system can adopt for sending & receiving information while ensuring that objectives set out to designate a successful exchange of message is addressed as well.

II. RELATED WORK

The Guidelines for Usage of Digital Signatures in E-Governance Version 1.0, says that the digital signature implementation must be end to end available, and the State Government should develop its own franchisee model for management of digital signatures on a day to day basis, else it may impede decision making. Organizations should not promote physical signatures on print outs of any DSC [7].

"For digital signature infrastructure to work effectively they require not only technological solutions but also an authoritative infrastructure" Says G.C Parry, M.James Moore, A.P Graves and O.Altinok In their research paper [8]. Their study clearly shows that the use and implementation of the digital signature is not very popular worldwide, because of lack of common legal base and many loopholes which are there in PKI implementation.

Hanna has conducted a survey and a follow up survey in June and August 2003, to identify the primary obstacles to PKI deployment and usage [9]. This study clearly shows that PKI is a horizontal enabling technology, and around 92% of the respondents agree to use PKI, if obstacles are removed. Major obstacles that were identified in the study are that the software do not support PKI, cost of implementation is very high and "one critical application

that needs improvement in PKI support is document signing".

Bergius Tulu, Haiging Li, Samir Chatterjee, Brian N Hilton, Deborah Lafky and Thomas A. Horan, in their research paper have given a solution for the implementation of Digital Signature solution for a health care enterprise [10].

According to "PKI standards and solutions for e-signatures" a white paper, organisations are reluctant to implement DSC because of complexity and cost of typical implementations of the digital signatures. PKI algorithms are often associated with lengthy deployments, high expenses and very difficult ongoing management for deployment beyond 100 users [11].

"People are naturally uncomfortable with change and PKI is not yet widely understood and it is not perceived as having demonstrated trustworthiness to deal with these concerns, agencies should develop a public information plan or comparable document covering the agency's design, implementation and presentation of the electronic application" says Kaathy Lyons Bruke, Federal PKI steering committee member[12].

III. PROPOSED TECHNIQUE

An issue which we found was more detrimental in promoting usage of PKI within Government environment was the mechanism of conveying entitlements when performing transactions in an heterogeneous environment where multiple independent systems work together to conclude a transaction. Though DSC could help verify the authenticity and the owner of the transaction, it does not have any capability to suggest whether the owner is actually entitled to perform the transaction. Verification of entitlement is an essential requirement within Government Business and ensuring this in an heterogeneous environment is a challenge and has not been tried earlier. Subsequent sections of this paper try to define a series of steps which can help ensure that interacting systems in a heterogeneous environment are easily able to establish the genuineness of a transaction both in terms of ownership as well as entitlement.

There are four key objectives which a message exchange has to address in order to conform as a reliable and successful exchange Non Repudiation, Authenticity, Confidentiality and Reliability. Given below are the detailed explanations about the ways these objectives would be achieved.

A. Non-Repudiation

A communication exchanged between two entities will be of relevance if both the parties engaged in the exchange are able to conclusively point the origin of the communication. In normal world this is achieved by the sender signing every communication sent out by him / her. By signing the communication the sender takes responsibility of the content shared through the communication. This assures the receiver that the content sent through the communication originated from the sender or the under-signed and that the sender hereafter will under no circumstances be able to repudiate the same.

In digital environment the same is accomplished using digital signature wherein the sender uses his private key to sign a document. The document can be verified by using the corresponding public key. Since there can be only one combination of private and public key as such only the corresponding public key can be used to verify the document signed through a particular private key. Since the private key is only available with the signee as such this system establishes the origin of the communication to correct entity. Such signatures are also accompanied with certificates from 3rd party certifying authority which conclusively establishes the identity of the sender.

Under IT Act 2000, Government of India has created the Controller of Certifying Authorities (CCA), CCA authorizes various agencies to act as a certifying authority (CA) and issue digital certificates to individuals and entities. CA through a registering authority (RA) verifies identity documents of individuals / entities and upon establishment of identity issues a digital certificate. Through such digital certificates CA commits to the fact that the identity of the owner of such certificate has been verified & established.

Each digital certificate will have two forms,

1. A certificate establishing the identity of the owner along with the owner's public key. Such a certificate can be easily verified by contacting the CA whose URL is embedded within the certificate. Such types of certificates would be circulated as a file and the extension of such files would be '.cer'. Such files will not contain the private key. This file will follow X.509 standard certificate format. This certificate will be circulated to all participating entities. Some key fields which would be part of such certificates are –
    - Validity period (from date and to date)
    - Name of the certificate owner
    - Email id of the certificate owner
    - Public key associated with the certificate
2. A password protected private key which will be kept separately and will be retained by the certificate owner. The extension of such files would be '.pfx' and such files would not contain the private key. Such files will follow PKCS #12 standard format.

The digital signing process will involve use of private key by the signee to sign the document he / she intends to share with a user in the participating entity. Upon receiving the signed document, the recipient will use the publicly available certificate of the signee to verify the authenticity of the signee and subsequently use the associated public key to validate the signature. The detailed sequence of steps which should be followed has been listed below –

Process Steps

Step 1. Issue of certificates from a registered certifying authority

All participating entities should get DSCs for them as well as for their employees issued from a Government

authorized CA. The series of steps which will be initiated in this regard are

Sub Step 1. Any authorized user wishing to have DSC will be provided with a login over CA website. Through this login the user will generate a Public-Private key pair required for digitally signing documents.

Sub Step 2. The user will also be provided with a USB Token from agencies such as Safenet, StarKey and Aladdin. The user will store his private key in this USB token.

Sub Step 3. The public key will be sent to CA for generation of certificate. In parallel CA will be sent a copy of the application form along with supporting documents.

Sub Step 4. Upon verification of all supporting documents and the application form CA will issue a certificate embedded with the public key of the user.

A copy of the certificate will be shared with Government Financial Organization, which will store it in its database. Validity of such certificate will be limited to two years. Please note that the certificate will come in the form of '.cer' and the private key will exist with user as '.pfx' stored in the USB token.

Step 2. Sharing of Digital Certificate (.cer files) containing the Public Key between participating entities

Once the certificate has been generated, the same has to be shared between participating entities. E.g. Government Financial Organization will share the certificates of its employees with agency banks, accountant general, etc. This sharing of data will be performed in the following manner –

Sub Step 1. The Government Financial Organization will identify all authorized designations, persons associated with these designations and their locations within the organization. These details will be packed with the corresponding public key certificate of the Organization's personnel.

Sub Step 2. The packed data will be signed by the organization using its own private key.

Sub Step 3. The signed set of information will be dispatched to the intended participating entity using a SSL channel.

Sub Step 4. The participating entity after verifying the signature will unpack the data and store the name, designation, location and public key certificate within its database. These details will be used by the entity in validating the sender of the information, his / her designation and location.

Step 3. Signing of documents for exchange

Once step 1 & 2 have been completed, the next logical action would be to initiate digitally signed communication. This would be done in the following manner –

Sub Step 1. The officer from the organization who intends to send some document such as payment instruction or mandate would generate the details to be signed from the organization.

Sub Step 2. He / she will sign the document using his / her private key stored in a USB token.

Sub Step 3. The signed document will be subsequently posted to the interface of the participating entity.

Step 4. Verification of signed documents

Upon receiving a document the participating entity will have to verify the authenticity of the communication. This process will involve the following steps –

Sub Step 1. The participating entity will see the message content for retrieving the nature of communication. E.g. the participating entity will check a payment instruction to verify the origin of the instruction, including the sender's name, designation, location & public key certificate id.

Sub Step 2. It will subsequently contact the organization's identity management server for verifying the existing signing authority for the communication received by it.

Sub Step 3. Participating entity, using the certificate id, will retrieve the certificate and corresponding details such as name, designation & authorized location.

Sub Step 4. Participating entity will check whether the name designation & authorized location retrieved from its own database matches with that which has been sent as part of the communication.

Sub Step 5. It also checks whether as per the organization's identity management server the sending person is currently authorized to sign the communication.

Sub Step 6. If the verification listed in sub step 4 & 5 concludes successfully then signature verification is initiated by extracting the public key from the certificate retrieved by the entity from its database against the certificate id communicated as part of the communication.

Sub Step 7. If the signature verification is successful in sub step 6 then the communication is accepted and an acknowledgement is sent back else the communication is rejected

and a corresponding message is sent back to the organization.

Step 5. Backup of .cer and .pfx files

A major requirement of a successful PKI model is that both the public and private keys are retained for a stipulated period of time. This is important since both these keys expire every 2 years and subsequently a new key pair is generated. Even after expiry it may be required that the signatures done using old pair are validated. This can only be done if the old pair is retained. The organization should ensure that upon expiry of a DSC, the same is backed up within a repository so that in the future the same information can be used to validate those documents which were digitally signed using the old pair.

Step 6. Periodic sharing of user detail modifications with participating entities

Sometimes many changes keep happening inside the Government department, for e.g. transfer of officials within the department to different post and location. Some new officers are also added because of new recruitment, deputation from other departments or promotions. Some officers move out because of retirement, death or external deputations. This would mean addition, modification or deletion to the list of public key certificates and corresponding details available with the participating entities. On every such change sub steps mentioned in Step 1 will be re-initiated.

Step 7. Renewal of DSC along with public-private key pair

As per statutory requirements the public-private key pairs have to be renewed every two years. The organization should create processes to support this process. A reminder service will be invoked to keep the organization's users informed about upcoming expiry of DSCs. The System Integrator will maintain a dedicated division looking after the management of DSCs, as a matter of practice it will ensure timely backup of expired DSCs and also replacement of the same with a new DSC.

The six step process defined above will be the essential element in ensuring non-repudiation.

B. Authenticity

Any government organization to use the model as stated above should have clear roles and associated responsibilities identified within the system. All activities within the system should be performed as per the roles assigned. While the organization should be performing all verification to ensure that authorized personnel are able to generate and share communication with participating entities. It is also desired that the participating entity is also able to verify whether the communication received by it was from sources that have been authorized to send communications of that nature.

Each communication sent should have a type which should be mapped with the allowed designation and the location associated with that designation. The organization should share with all participating entities the list of all communication types mapped with names of individuals having rights to send such communications to the entity. Also associated would be the designations of such individuals and the locations for which the individual is authorized to sign and communicate.

The activity of sharing these details would be done in three steps. First step will see communication of one-time information about such individuals, the second step would be real-time communication of changes in roles & responsibilities and the third step would be periodic communication of long term changes in roles & responsibilities. These three steps has been listed below –

Process Steps

Step 1. Sharing of communication types and associated authorized personnel details with participating entities

During commencement of operations between the organization and other participating entities, an initial package of information about types of communication to be expected from the organization and the details of authorized personnel allowed to communicate with them would be shared with participating entities. This sharing of data will be performed in the following manner –

Sub Step 1. The organization should identify all types of communications to be shared with the concerned participating entity. It should also identify concomitant authorized designations, persons associated with these designations and their locations within the organization. These details will be packed with the corresponding public key certificate of the Treasury personnel.

Sub Step 2. The packed data will be signed by the organization using its own private key.

Sub Step 3. The signed set of information will be dispatched to the intended participating entity using a SSL channel.

Sub Step 4. The participating entity after verifying the signature of the organization will unpack the data and store the communication types along with associated personnel name, designation, location and public key certificate within its database. These details will be used by the entity in validating the sender of the information, his / her designation and location in order to verify whether the sender is authorized by the organization for sending the communication of that nature.

Step 2. Verification of signed documents for authenticity

Upon receiving a document the participating entity will have to verify the authenticity of the communication. This process will involve the following steps –

Sub Step 1. The participating entity will see the message content for retrieving the nature of communication. The first check would be to see the type of communication which has been received. E.g. For agency

banks the types of communications they can expect would be challan details, payment instructions, memorandum of errors, VDMS, pension payment orders, etc.

Sub Step 2. Each type of communication can only be done by authorized personnel. This detail would be available both in participating entities database as well as in the message content. E.g. the participating entity will check a payment instruction to verify the origin of the instruction, including the sender's name, designation, location & public key certificate id. The details provided in the message content and that stored in the entities database should corroborate.

Sub Step 3. It will subsequently contact the organization's identity management server for verifying the existing signing authority for the type of communication received by it. The entity will share location and communication type details with the server and server will return the personnel name, his / her public key certificate id and his / her designation.

Sub Step 4. Participating entity, using the certificate id, will retrieve the certificate and corresponding details such as name, designation & authorized location from its own database. It will also retrieve the type of communication the personnel is authorized to make.

Sub Step 5. Participating entity will check whether the name designation & authorized location retrieved from its own database matches with that which has been sent as part of the communication.

Sub Step 6. It also checks whether as per the organization's identity management server the sending person is currently authorized to sign the communication.

Sub Step 7. If either of the verification listed in sub step 4 & 5 concludes successfully then signature verification is initiated by extracting the public key from the certificate retrieved by the entity from its database against the certificate id communicated as part of the communication.

Sub Step 8. If the signature verification is successful in sub step 7 then the authenticity of the communication is successfully established.

Step 3. Periodic sharing of user detail modifications with participating entities

Most of the government organizations see changes resulting from transfer of officials within the department to different posts and location. Some new officers are also added because of new recruitment, deputation from other departments or promotions. Some officers move out because of retirement, death or external deputations. This would mean addition, modification or deletion to the list of authorized personnel having rights to send various types of communications. On every such change sub steps mentioned in Step 1 will be re-initiated.

C. Confidentiality

Sometimes organizations have to share sensitive details with participating entities such as agency banks. These details are sensitive in nature and should be received by intended recipients only. Unauthorized persons should not even be able to view the data.

For such scenarios Secured Sockets Layer (SSL) technology can be used to ensure information confidentiality. SSL would supplement digitally signed documents by providing them with a platform for sharing data through an encrypted path. Thus a system would be created wherein non-repudiation would be supplemented with encryption.

Using of SSL would require both the organization and participating entities to procure a server certificate and a public-private key pair. Each institution can have only one certificate. This certificate will be used to establish the identity of each system before initiation of a communication between two systems. The steps associated with ensuring confidentiality of information during data exchange between the organization and a participating entity is listed below –

Step 1. Procure SSL certificates from CA

Step 2. Deploy SSL certificate in the servers

Step 3. Publish URLs

Step 4. Authenticate the partner

D. Reliability

Reliability can be ensured by following a three-step handshaking protocol. The objective of the protocol would be to negate the following possibilities –

1. Tampering of information during transmission.
2. Transmission of incomplete information.
3. Failure of transmission of information.

The three steps of the handshaking mechanisms are listed below –

Step 1. Create SSL channel by pro-active authentication

Step 2. Communication of digitally signed information

Step 3. Sending back the digitally signed acknowledgement

Upon receiving the information, the receiving partner in the communication will create a hash of the data received and will subsequently encrypt the same using the entity's own private key. This encrypted hash will be sent back as an acknowledgement of successful receipt of the

information. Upon receiving the acknowledgement the sending entity will perform the following sub-steps –

Sub Step 1. It will create hash of the data originally sent by it and match it with the encrypted hash sent back to it by the receiving entity. This will be done after decrypting the received hash using the public key of the receiving entity.

Sub Step 2. In case the matching is successful then the sending entity will record the transaction transmission within its database as successful. In case the matching is not successful then a re-transmission of message will be attempted based upon the type of error reported.

Sub Step 3. It may also happen that the intended recipient did not receive the message in the first place. Under such circumstances no acknowledgement will be sent, instead after expiry of the timer mentioned in step 1, the intended recipient will initiate a message to the calling entity informing it about its failure to send the message. The calling entity will re-send the message. In case even after resending the message the intended recipient did not receive the message then all steps from step 1 onwards will be re-initiated. Such attempts will be made for 2 times, after which the system will escalate the issue to technical team for appropriate action.

Sub Step 4. In case of scenario where acknowledgement was sent by recipient after successfully receiving the message but the same did not reach the sending entity; under such circumstances the sending entity will resend the message along with the old transaction id, upon expiry of the timer mentioned in step 2. The receiving entity will be responsible for checking whether the transaction id of the newly received message corresponds to any older message received previously. In case if such relationship is established then the recipient will send back an acknowledgement without re-processing the message again. In case if the new message does not correspond to any old message then the recipient will process the message and send an acknowledgement back to the sending entity. In case acknowledgement is still not received by the sending entity then the problem will be escalated to the technical team.

The steps mentioned above will help establish reliability within communication between the organization and all participating entities.

IV. CONCLUSION

Adoption of PKI enabled DSC systems have been limited within the Government Businesses. The paper was an attempt to analyze the reasons for such limited adoption and find out a strategy to promote greater acceptance to PKI so as to ensure migration of Government Businesses from paper based workflow to digital workflow. Challenges which we listed, varied from commercial reasons to statutory challenges. While commercial factors are beyond the scope of this paper, we tried to address concerns which lead to statutory challenges.

A prime concern we saw was the communication of the information about entitlement of the signee to sign a transaction. In a standalone environment such as e-filling systems for MCA21, Income Tax Department or e-Submissions for e-Procurement systems, managing entitlement data along with the associated DSCs are easy. But in an environment where multiple independent systems talk to each other and each system receives signed document from authorized users of the other system, it is very difficult to ensure that recipient system is able to verify the entitlement of the signee of all communications received by it.

The paper attempted to solve this riddle. The approach taken in this paper has been to identify essential requirements of a reliable and successful message exchange and create a step by step walkthrough simulating scenarios of interaction. We hope that the paper has been able to derive a possible algorithm which can be followed to ensure communication of entitlements to all participating entities within a transaction. We also hope that Government departments will find this algorithm acceptable and use it to migrate their paper based workflows to digital workflows, thus ensuring greater transparency and accountability within their working culture, which we feel is greatly required within various backward and emerging economies.

REFERENCES

[1] IT ACT 2000 Available: http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf. Page no. 2, 4-13

[2] IT Act 2008 Available: http://bsu.bih.nic.in/%28S%28ff3tcebmkoyb1h55i1x3v145%29%29/static/downloads/itact/it-amedment-act-2008.pdf Page no: 5, 17,18

[3] "Guidelines for Usage of Digital Signatures in E-Governance Version 1.0", Department of IT, Ministry of Communications, and Information Technology, GOI Available : www.icisa.cag.gov.in/images/Guidelines_for_Usage_of_Digital_Signatures_in_E-Governance_Ver.1.0.pdf.

[4] "Legal aspects of electronic signatures" by G.C Parry, M James Moore, A.P Graves and O.Altinok Available "www.bath.ac.uk/management/research/pdf2008-02.pdf".

[5] Hanna S(2003) " Obstacles to PKI deployment and usage - survey results and draft action plan", Proceedings of fifty eight Internet Engineering Task Force, Minneapolis, MN, USA.

[6] "Design and Implementation of a digital signature solution for a healthcare enterprise" by Bengisu Tulu, Haiging Li, Samir Chatterjee, Brian N Hilton, Deborah Lafky, Thomas A Horan" Available:www.cgu.edu/pdffiles/KayCenter/amcis2004.pdf.

[7] "PKI Standards & Solutions for Electronic Signatures" Available www.arn.com/resources/white-papers/pki-solution-for-electronic-signatures.htm

[8] "Federal Agency use of PKI for Digital Signatures & Authentication" by Kaathy Lyons-Bruke(Federal PKI Steering Committee), NIST special Publication, Available www.csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf.