An Approach towards Digital Signatures for e-Governance in India

Vijay Jain
C-DAC Mumbai,
Gulmohar Cross Road No: 9,
Juhu, Mumbai-50, India
+912226201606
vijayj@cdac.in

Ranjan Kumar
C-DAC Mumbai,
Gulmohar Cross Road No: 9,
Juhu, Mumbai-50, India
+912226201606
ranjank@cdac.in

Dr. Zia Saquib
C-DAC Mumbai,
Gulmohar Cross Road No: 9,
Juhu, Mumbai-50, India
+912226201606
saquib@cdac.in

ABSTRACT
Recent development in the area of e-Governance would like to leverage Digital Signature capabilities, but facing challenges due to lack in user expertise, technology and procedural challenges associated with it. Recently in India, the Government has taken various initiatives under Digital India program to completely enable e-Government transactions in an online mode. Initiatives taken by the Government are supposed to reduce the physical movement of papers, while interacting within all target groups (Government, Citizen and Businesses) in a secured and transparent manner. Digital Signature as part of Public Key Cryptography is a well-known mechanism to achieve digital authentication and verification of electronic transactions in the online world. This paper discusses one of such initiative taken by the Government for enabling e-Authentication and Security in the Transaction Phase of e-Governance in India. This paper also describes Service Oriented Architecture (SOA) based Signature Service Middleware (SSM), to realize digital signing of transactions in the e-Governance. SSM is currently in prototype stage.

Categories and Subject Descriptors
E.3 [**DATA ENCRYPTION**]: Public key cryptosystems; H.3.5 [**Online Information Services**]: Data Sharing, Web-based services; J.1 [**ADMINISTRATIVE DATA PROCESSING**]: Government

General Terms
SECURITY, HUMAN FACTORS, EXPERIMENTATION, DESIGN

Keywords
Cryptography, Mobile Digital Signature, Digital Signing, One Time PKI, Asymmetric Cryptography using Mobiles, Transaction based Digital Signature, Digital India, Cloud Digital Signature, and Cloud Computing

1. INTRODUCTION
Gartner, an international consultancy firm has formulated four phases of e-government model [1] and are depicted in figure 1.

Many of the e-Governance initiatives in India have crossed Interaction phase and are moving or already moved into a Transaction phase. As it can be seen in the figure 1, e-Authentication and Security are key factors to accomplish success in the Transaction phase. To enable e-Authentication and security, Indian Government has taken various initiatives across all interaction groups within the government such as, Government to Citizen (G2C), Government to Business (G2B) and Government to Government (G2G).

Cost effective Digital Signature for e-Governance will empower e-authentication and digital signing across online services in G2C such as filing of income-tax, property-tax, renewal of licenses, visa and passport issuance, etc. G2B services alike e-Procurement, applying for company registration, etc., and G2G services such as e-Office where intra or interdepartmental communication needs to take place.

Recently in India, the Government has taken various initiatives under Digital India program to completely enable e-Government transactions in an online mode. Initiatives taken by the Government are supposed to reduce the physical movement of papers, while interacting within all target groups (Government, Citizen and Businesses) in a secured and transparent manner. One of such initiative by the Indian Government is Digital Locker [5], where Government has targeted a complete transformation of paper documents into digital documents. Through Digital Locker, the Government is trying to automate the complete e-document life cycle starting from document generation, its issuance/ re-issuance, usage, cancellation/expiration and sharing of them among the various stakeholders. To accomplish and complete the whole transaction online in a secured manner, the Government has also introduced a Digital Signature service, eSign [6]. eSign is a cloud based signature service, where various e-Governance as well as non e-Governance applications can offer a digital signing of the documents to Aadhaar [7] holders. eSign facilitates digital signing using an open Application Programming Interface (API) [11]. eSign uses Aadhaar authentication [8] and e-KYC [9], an authentication mechanism offered by the Unique Identification Authority of India (UIDAI) [7], to complete the online identity verification of the users. At present, Digital Locker is availing e-Sign facility for digital signing of the documents by the Aadhaar holders.

This paper discusses one of such initiative taken by the Government for enabling e-Authentication and Security in the Transaction Phase of e-Governance in India. This paper also describes another Service Oriented Architecture (SOA) [10] based Signature Service Middleware (SSM), to realize digital signing of transactions for e-Government. SSM is currently in prototype stage. The paper is organized as follows. Section 2 describes the e-authentication and security. In section 3, the implementation of the eSign is being explained. Section 4 describes about Signature Service Middleware (SSM). Finally, Section 5 presents the conclusions.

2. E-AUTHENTICATION AND SECURITY
The core of the authentication / security system is to uniquely identify the users. This is being achieved in India through Aadhaar project, which provides the unique identity number to each resident of India. Currently, Aadhaar system has a centralized database of around 0.9 billion of unique identity numbers and stores demographic as well as biometric data of the Indian residents.

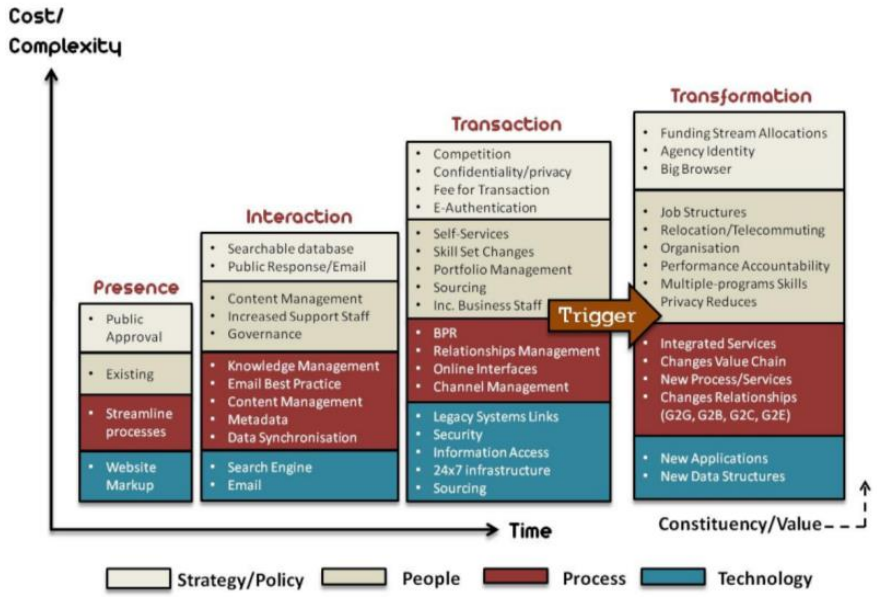

Figure 1: Four Phases of e-Government [1]

On top of this database, UIDAI, which is the nodal agency for this database, provides authentication [8] and e-KYC [9] services.

Various governments in the world have been playing an authoritative role in identity provision in the physical world and are now faced with demands to establish digital identities in order to support e-Government initiatives in an online manner. It is the role of the government to associate digital identities of specific person, who will be authorized to perform certain actions in physical or digital forms. Digital signature helps in proving individual's digital identity. This digital identity consists of two parts 1) private key that is used for creation of digital signatures and proves the ownership of the public key 2) a public key embedded within a Digital Certificate and can be used by anyone to verify the digital signature.

2.1 Public Key Infrastructure

Digital Signature as part of Public Key Cryptography is a well-known mechanism to achieve digital authentication and verification of electronic transactions in the online world. According to Bellare and Rogaway [2], a cryptosystem is in general a pair of algorithms that uses a key to convert a plaintext to cipher text and vice versa. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third-party validation authority (VA) can provide this information on behalf of the CA. Encryption is a technique in which a message is transformed into non-readable form and can only be known to the sender and receiver of the message. Digital signature in contrast to paper based signing not only provides data security but also maintains digital integrity [4] for signed transactions. Authentication [3], where verifying the identity of the information sender and the receiver is important and can also be achieved using Digital Signature in the online world.

In e-Governance context the signed transaction either by the Government or user can easily be verified at the other end using an embedded public key in it. An encryption can also be achieved using public key of the government department which is offering the online service. A message encrypted with a public key of the government can only be decrypted by the government. Given a key pair, data encrypted with the public-key can only be decrypted with its private key; conversely, data signed with the private-key can be verified with its public key. This characteristic is used to implement encryption and digital signature in the e-Governance. This encryption and digital signing ensure transaction privacy as well as non-repudiation during its transmission between G2C, G2B and G2G.

In India, Digital Signature means authentication of any electronic record by a subscriber by means of the procedure specified in Section 3 of the IT Act, 2000. Controller of Certifying Authorities (CCA) [12] is the supreme body in India who exercises supervision over the activities of Certifying Authorities (CAs) and certifies the public keys of certifying authorities. The Certifying Authorities are granted license under the IT Act, 2000 by the Controller to issue Digital Signature Certificate (DSC).

Any user can make an application to licensed CA for issuance of DSC in such form as may be prescribed by the Government. For issuance of DSC, the applicant's personal identity, address and other details get embedded in the DSC and need to be verified by the CAs against an identity document.

Digital Signatures are widely used for authentication in the electronic environment. Providing cost effective Digital Signature service in an effective manner faces challenges due to lack of user expertise, technology and procedural challenges associated with it. To overcome such issues cloud based digital signature can be seen as a model for reliable, convenient, on demand network access security infrastructure that performs cryptographic operations of Digital Signatures [25, 26]. Indian Government has introduced such a cloud signature service, eSign. eSign service follows Transaction based digital signing as compared to cloud service described by Wojciech [13].

3. DIGITAL SIGNING USING CLOUD INFRASTRUCTURE

Storing private keys, in the cloud, using the several key recovery agents is being proposed by Anderson et al. [15]. To increase usage of Digital Signature without compromising security aspects [23] a cloud based Digital Signature services are becoming popular. Another cloud based service using a proxy service to HSM is being described by Wojciech [13]. eSign, a cloud based Digital Signature service by Indian government also achieves the same in One Time PKI mode by generating the user's key pair in the cloud infrastructure using a Hardware Security Module (HSM). eSign offers transaction based DSC issuance, i.e. One Time PKI. In One Time PKI user's Public-Private key pair is generated in the cloud and will only be valid for signing of a single transaction. Whereas in the longer validity DSCs, single DSC can be used to sign multiple transactions. In eSign, HSM not only generates and stores the private key, but also used for secure signing of the document on behalf of the user. User's generated private key never leaves the HSM. HSM is a certified [16] tamper resistant Hardware Security devices to carry out the cryptographic operations. In eSign, the user is issued with DSC based on online identity verification using Aadhaar e-KYC [9]. It is being proposed by the CCA [12] that eSign infrastructure should be owned by trusted third party. CA acts as the trusted third party and being trusted by both the owner and the verifier of the Digital Certificate. Consent of the user is important because the key pair is generated on the premises where the user has no control. This consent step is critical because signing is done by trusted third party on behalf of the user based on the electronic verification of the user. In traditional DSC issuance CAs has to carry out user identity verification in some manner before issuing the Digital Certificate. This identity verification can either be through online identity databases such as e-KYC service, provided by UIDAI, or considering mobile number, any other verifiable identity number to complete the identification process. According to eSign gazette notification* [17], this e-KYC service can fulfill the pre-requirement of verification of the applicant's personal identity for the issuance of the Digital Certificate, provided the conditions mentioned in the gazettes are met. After completing user's online identity verification using e-KYC [9], Key pair and Certificate Signing Request (CSR) [18] gets generated in the eSign HSM, and generated CSR is sent to the CA for issuance of the DSC. Entities which are involved in completing the digital signing are described below:

A. ***Application Provider*** **-** Application Providers are the government or non-government entities which would like to accomplish the digital signing of transactions using a cloud based infrastructure for Aadhaar holders. Application Providers will use the eSign service for providing Digital Signature facility for its users. Digital Locker [5] acts as an Application Provider for the eSign and consumes eSign API to facilitate Digital Signature to its users.

B. Digital Signer: Signer i.e. a user of the Application Provider. User here acts as the digital transaction signer and provides authorization to proceed with the signing of the particular transaction. For eSign, users are supposed to hold a valid unique identity number, termed as Aadhaar Number and issued by the UIDAI [7].

C. ***eSign Provider*** **-** e-Sign Service Provider acts as the signature service provider and carries out user's online identity verification, generation of key-pair in the cloud and requesting a DSC from the CA and the signing of the user authorized transaction. eSign Provider receives input from the Application Provider as per the protocol specified in e-Sign API [11]. eSign Provider invokes the user's online identity verification using Aadhaar data provided in the input. eSign uses HSM to perform the cryptographic operations. eSign Provider provides an API and can also provide web interface, as provided by the Application Providers to its users for carrying out a digital signing of the transaction. e-Hastakshar [28] acts as eSign provider as well as providing a web interface for carrying out digital signing of transaction in India.

D. ***Certifying Authority (CA)*** **-** CAs is granted license under the IT Act, 2000 by the CCA [12] to issue DSC [8]. In this whole infrastructure CA in conjunction with eSign Provider receives the CSR [18] from eSign for online generation and issuance of DSC.

E. ***Identity Verification Service Provider*** **-** In India, UIDAI provides an online database of its residents (user) for identity verification purpose. UIDAI which holds demographic and Biometric data of the user issues a unique identity number termed as Aadhaar Number to the user. Any government or non government entity interested in carrying out the online identity verification can use the authentication and e-KYC service offered by the UIDAI through a Representational State Transfer (REST) [29] protocol based Web Service API. Details about the protocol and procedural requirements to perform authentication and e-KYC can be read from the UIDAI API [8, 9] documents.

To digitally sign a document the following steps are being followed:

- Functionality performed by the eSign involves the validation of the incoming request, digital integrity verification of the input against the Application Provider (AP) public certificate.
- e-Sign service after successful completion of validation and digital integrity of received XML message as per the eSign protocol, forwards the Aadhaar authentication data, which was part of the e-Sign request to Aadhaar service for e-KYC purpose. Aadhaar e-KYC service receives the input format as per the e-KYC API [19]. e-KYC is carried out by the Aadhaar service and the response, whether successful or unsuccessful is returned to the e-Sign service.
- On successful e-KYC, e-Sign Provider generates a Key pair and a CSR. e-KYC data provided by UIDAI contain user's demographic information, and utilized for creation of CSR [18] and created CSR is then sent to the CA for the generation of DSC for the user.
- On receiving a DSC from the CA, eSign creates a Digital Signature using 1) message digest: The message digest is a representation of the original message to a unique 160-bit string of characters. This 160-bit Hash created for a transaction has always been unique, i.e. no two messages will have the same message digest unless they are absolutely identical and once generated are non-convertible into the original message. This transaction or document Hash is provided by the Application Provider in the input. 2) Digital Signature creation using Hash of a transaction: Digital Signature creation is achieved by encrypting the generated message digest with the Digital Certificate owner's private key. Original message using which message digest is being created gets supplemented with Digital Signature and the owner's public certificate and returned as a signed message to the Application Provider. This signed message can easily be verified at the Application Provider end using the embedded public key in it.

Figure 2 demonstrates the flow diagram for Digital Signature using the eSign provider.

*Current gazette only legalize the transaction based, i.e. One Time PKI with generation of key pair in the cloud.

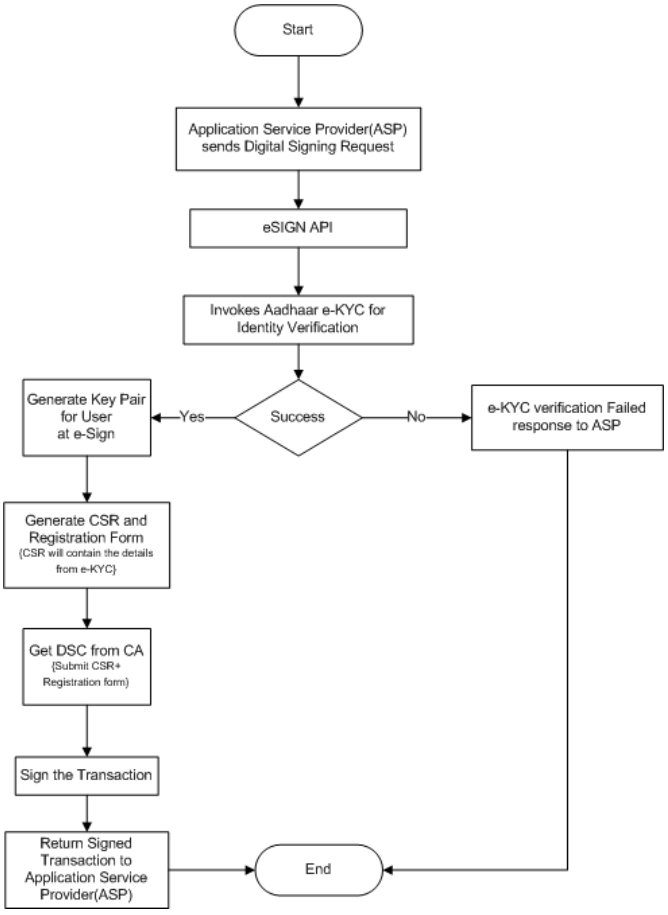

Figure 2. eSign Service Work Flow

4. DIGITAL SIGNING USING SIGNATURE SERVICE FRAMEWORK

Recent developments in the cryptography have provided various platforms for digital signing of the transaction. It has been observed that there are ways to achieve the digital signing of the transaction using 1) Cloud Infrastructure i.e. Private-Public key pair gets generated in the cloud and does not remain in the possession of the user. This infrastructure can be used to generate a typical Digital Signature or can also support One Time PKI, as already realized in eSign. Cloud infrastructure has to be secured enough or security attack resistant to avoid the threat to the user's private key. 2) Non-cloud infrastructure, i.e. key pair generation takes place in the security token in conjunction with mobile or web. This security token remains in the possession of the signer (user) of the transaction. There are lot of development in creating a Digital Signature in the last decade and mobile as well as web is being considered as one of the digital signing mediums to generate and use the Digital Signatures. Technologies to create and use Digital Signature in mobile device ranges from SIM based solution to a service based solution. Detailed advantages and disadvantages of each approach are being discussed by the author [20]. Secure Digital Signature creation environment, based on mobile devices and smart cards, is defined and analyzed by A. Mana et al. [14]. The private key of user can also be stored on the SIM cards as suggested by H. Rossnagel [21]. In web USB and smart card security tokens are utilized to achieve the digital signing of the transaction. In cloud based Digital Signature, private key of the user remains in the control of the Digital Signature service provider and security of cloud based Digital Signature system depends upon the protection of user's private key from being misused without user's authorization. It is alike storing of a user's valuables in the bank locker. In existing studies, we observed that the Application Providers, i.e. the entities which are in need of Digital Signature services are left with limited options of choosing the Signature service either cloud based or non-cloud based. Similarly, a concept of One Time PKI, which was not visualized in the earlier cloud as well as non-cloud infrastructure, is now being provided using eSign in India. To overcome such limitations and providing more choices to the Application Provider as well as to the user's of those applications, Service Oriented Architecture (SOA) [10] based Signature Service Middleware (SSM), is suggested in this paper. This SOA based SSM can be considered as an integrated framework to support both Cloud as well as Non-Cloud infrastructure based digital signing. SSM can also support the concept of One Time PKI as being supported in the eSign. In this paper basic model of Digital Signature service using SSM is presented. Detailed design, architecture and protocol details for SSM are being kept outside the scope of this paper. SSM protocol is being designed keeping in view to support the Digital Signature using multiple signing mediums, such as mobile, web and cloud. In SSM ecosystem entities which are being considered to complete the digital signing of the transactions are described below:

A. Application Provider **-** Application Providers are the government or non-government entities which would like to accomplish the digital signing of transactions. Signer i.e. user of the application will be provided an option of choosing a type of signing medium using which they can complete their transaction. Application Providers will use the SSM service and the options provided by it to facilitate Digital Signature to the end users. In eSign, Application Providers facilitate digital signing using eSign service. It is up to the Application Provider to allow users to choose the signing options or can be restricted based on the sensitivity of their applications. For example, an application requiring digital signing using only mobile and crypto token can show that option to its user on the application web interface. This way Application Providers can also choose the signing medium which they would like to allow for their applications.

B. Digital Signer: Signer i.e. a user of the Application Provider. User and signer terms are used interchangeably and provide authorization to proceed with the signing of the particular transaction. Signer initiates a transaction on the web interface provided by the Application Provider and proceeds with Digital signing of it using any of the signing mediums as provided by the SSM and supported by the Application Provider.

C. Signature Service Middleware **(SSM) -** SSM provides a Web Service API to the Application Providers and facilitates Digital Signature for the user's of the Application Providers. A protocol designed by the SSM will facilitate Digital Signature using Mobile, Web or Cloud. In mobile, Digital signing can be achieved using a mobile application and cryptographic security tokens. Similarly, on the Web it can be achieved by using Java Applet & security tokens. Digital Signature using Java Applet is also being proposed by Centner [22]. Private key remains in the possession of the user either by using a mobile application in conjunction with security tokens meant for the mobiles such as smart SD cards, SIM cards, software cryptographic libraries or utilizing USB, Smart Card based crypto token meant for web based applications. Security tokens used with mobile application can be

used to generate the Private-Public key pair, CSR [18] and requesting a DSC from the SSM. SSM protocol also provides an option where the user if does not want to carry out the Digital Signature using security tokens with Mobile or Web can opt for Cloud based key pair generation, similar to other Cloud based Digital Signature services as discussed in Section 3. SSM also supports verification of the signed transaction either through the Online Certificate Service Protocol (OCSP) [23] or using Certificate Revocation Lists (CRL).

D. Certifying Authority (CA) - CAs is granted license under the IT Act, 2000 by the CCA to issue DSC. In this whole infrastructure CA in conjunction with SSM Provider receives the CSR [18] from SSM for online generation and issuance of DSC.

E. Signing Medium: A mobile application installed on the user's mobile device will be used to generate the key Pair, CSR and getting of a DSC from the CA through SSM. Mobile application in conjunction with cryptographic security tokens achieves the digital signing using a mobile device. Cryptographic security tokens are equivalent of HSM in small sizes or in the form of Cryptographic libraries. These security tokens are supposed to manage the cryptographic keys and carrying out cryptographic operations. Managing private key in the security tokens brings its possession to the signer i.e. to the user. Java applets along with cryptographic USB, Smart Card can also be used to achieve the digital signing using web applications.

F. Security Token: Security tokens are usually designed as tamper-resistant and it is difficult to steal the information stored in them. In a public key cryptography, security tokens are primarily responsible for Key-Pair Generation, Certificate Signing Request (CSR) [18] generation and signing of the transaction. Mobile or Web Applet in conjunction with security tokens achieves the digital signing of the transaction and ensures the possession of the private key to the signer.

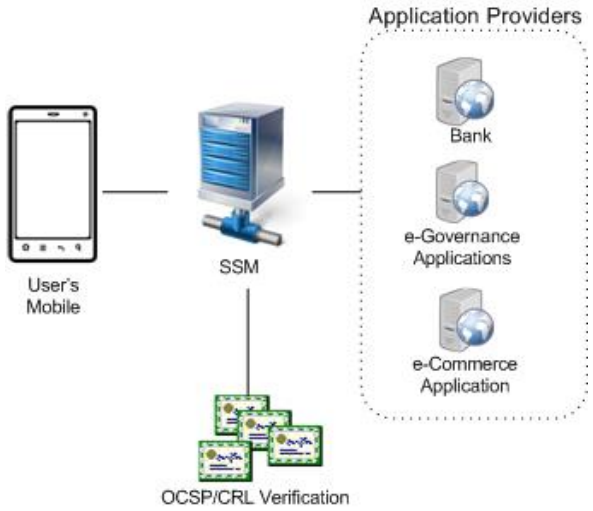

Figure 3. SSM Entities

Signature Service Middleware (SSM) is an intermediary service between Application Provider, which requires transaction to be digitally signed by the end-user using a mobile device, web applet or cloud infrastructure. SSM provides a SAO oriented web service interface supporting REST based communication over HTTPS. Identity verification for the purpose of issuance of DSC either for One Time PKI or non One Time PKI can either be carried out through online identity databases such as e-KYC [9] provided by UIDAI, considering mobile number as an identity, or any other verifiable identity number to complete the identification process. In this paper, we have described the digital signing flow using mobile device in conjunction with software based crypto token, Network Security Services (NSS) [27] and considering mobile number as an identity. NSS is open source FIPS compliant library for carrying out cryptographic operations. Signer uses its mobile device to complete the digital signing of the transaction. In the overall context the message Hash, that need to be signed will be provided to SSM by Application Provider, similar to what is being achieved in the e-Sign. This message Hash can be signed using a mobile device, rather than signing it in the cloud infrastructure. SSM will forward the request to a user's mobile device as received from an Application Provider. SSM provides a web service API for Mobile Application Registration, Digital Certificate generation for One Time PKI, non One Time PKI and Digital Signature verification of the signed transaction. Entities for SSM can be seen in figure 3.

Steps to enable Digital Signature with SSM using a mobile device are being described below:

1. The user has to initiate the digital signing transaction at Application Provider by choosing the available signing medium option and the generated request as per the XML structure defined by the SSM protocol will be sent to the SSM.
2. SSM notifies the mobile application by sending the SMS to the mobile phone that the signing request has arrived. It is necessary that mobile application should have registered either with Application Provider or SSM.
3. Based on the type of Certificate to be used as mentioned in the signing request by the Application Provider, the mobile application will either use the pre-stored Digital Certificate in the security token or will request a Digital Certificate from SSM.
    a. Request One Time PKI Digital Certificate from SSM
        i. The mobile application will generate a key pair in the crypto token and will request for a new certificate by sending a CSR to SSM.
        ii. SSM may carry out the identity verification before forwarding a request to a CA for DSC generation.
        iii. SSM receives the DSC from the CA and send it to the mobile device.
    b. If the signing request specifies the time based DSC, then the mobile application will invoke the pre-stored licensed CA issued DSC from the security token.
4. Mobile will sign the message Hash as received in Step 3.
5. Mobile will send the signed response to SSM
6. SSM will verify the signed response and will also verify the certificate sent by the Mobile through OCSP [23] / CRL.

SSM will notify the Application Provider about the status of the transaction, i.e., successfully verified or not along with signed response. Based on the result received from SSM, Application Provider can take a further action as per their application flow. Flow Diagram for Digital signing using SSM is demonstrated in Fig. 4.

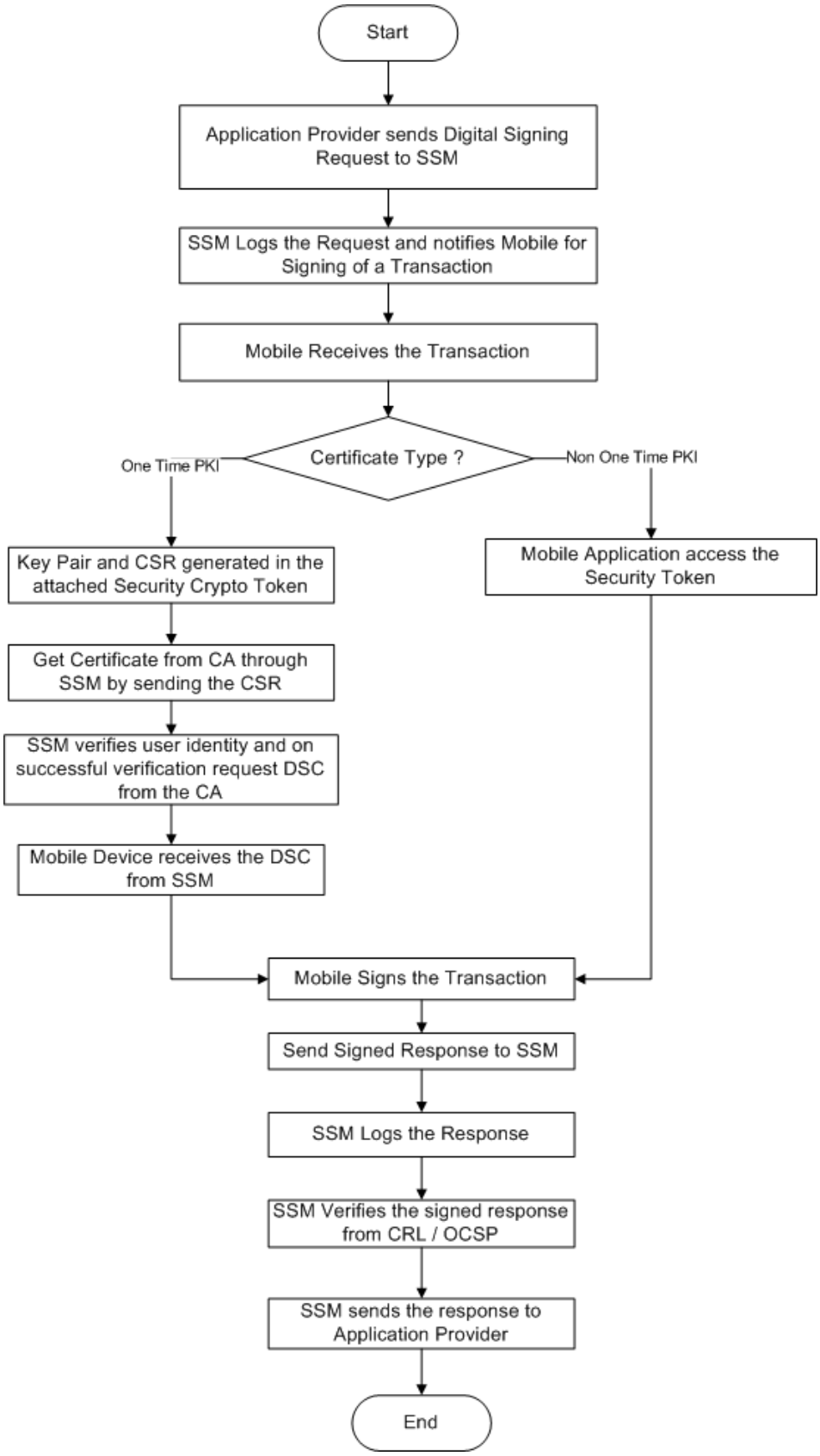

Figure 4. SSM Workflow with Mobile as a Signing Medium

5. CONCLUSION AND FUTURE WORK

SSM provides Digital Signature capabilities to the Application Providers which would like to avail the Cloud and Non-cloud infrastructure based digital signing. SSM capabilities for providing transaction management, auditing, and DSC issuance and signed message verification make it as an independent system to integrate with the G2G, G2C and G2B services requiring digital signing. SSM has already been prototyped using Non-cloud infrastructure using mobile and web. In mobile device, mobile application along with the NSS [27] crypto library is being used for prototype purpose, whereas for web, Java applet with USB crypto token is being tested. EJB-CA [24], an open source CA is being considered to test the prototype for One Time PKI using mobile application and NSS crypto library in the mobile. A support for Cloud infrastructure and encryption techniques to provide extra security for the message transmission over HTTPS among SSM, Application Providers and signing mediums are under consideration. SSM is being built using open source technologies and demonstrates potential of open source technologies for developing such a comprehensive system. By providing SSM as an integrated framework, we have tried to achieve the cost effective Digital Signature for G2G, G2C and G2B transactions. Cloud and Non-Cloud Infrastructure based digital signing and One Time PKI has its own advantages and disadvantages, which are being researched separately by the authors of this paper. A word transaction is being used throughout the paper to consider either a digital signing of a document or a challenge for the purpose of secure authentication.

6. ACKNOWLEDGMENTS

We are thankful to all the members of Software Engineering group of C-DAC, Mumbai for their direct as well as indirect contribution for this paper. We would like to pay our special thanks to Mr. Satish, Mr. Mayank Sachan, Mr. IK Mahesh, Mr. Shrikant Karwade and Ms. Shraddha Bhardwaj for helping out in the implementation of SSM POC.

7. REFERENCES

[1] Baum, C., & Maio, A.D. (2000) Gartner's four phases of e-government model. *Gartner Group Inc.*, Stamford.

[2] M. Bellare and P. Rogaway. *Introduction to modern cryptography*, 2005.

[3] M. Bishop. What is computer security. *IEEE Security Privacy*. Volume 1 Issue 1, pp. 67–69, 2003.

[4] G. J. Simmons. Symmetric and asymmetric encryption. *ACM Computing Surveys.* Volume 11 Issue 4, pp. 305–330, 1979.

[5] https://digitallocker.gov.in/

[6] http://www.cca.gov.in/cca/?q=eSign.html

[7] https://uidai.gov.in/

[8] https://uidai.gov.in/auth.html

[9] https://uidai.gov.in/fi-e-kyc.html

[10] https://en.wikipedia.org/wiki/Service-oriented_architecture

[11] http://www.cca.gov.in/cca/sites/default/files/files/eSign-API%20v1.0.pdf

[12] http://www.cca.gov.in

[13] Wojciech Kinastowski. Digital Signature as a Cloud-based Service. *The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING)*. Volume 1, pp. 68-72, 2013

[14] A. Mana and S. Matamoros. Practical Mobile Digital Signatures. *Proceedings of the Third International Conference on E-Commerce and Web Technologies(EC-WEB).* Sep. 2002, spp. 224-233.

[15] J. Anderson, F. Stajano. On Storing Private Keys 'In the Cloud' Extended Abstract. http://www.cl.cam.ac.uk/~jra40/publications/2010-SPW-key-storage.pdf [retrieved: March 2013].

[16] Security requirements for cryptographic modules, FIPS PUB 140-2, NIST, Dec. 2002.

[17] http://www.cca.gov.in/cca/sites/default/files/files/eSign_gazette_notification.pdf

[18] https://en.wikipedia.org/wiki/Certificate_signing_request

[19] https://authportal.uidai.gov.in/static/Authentication%200032%20-%20e-KYC%20API%20Document%20Version%201.0.pdf

[20] Antonio Ruiz-Martínez , Daniel Sánchez-Martínez , María Martínez-Montesinos and Antonio F. Gómez-Skarmeta. *A survey of electronic signature solutions in mobile devices. J. Theor. Appl. Electron. Commer*. Res. 2, 3 (December 2007), 94-109.

[21] H. Rossnagel. Mobile Qualified Electronic Signatures and Certification on Demand. *Proc. 1st European PKI Workshop Research and Applications*. Jun. 2004, pp.274-286.

[22] M. Centner, C. Orthacker and W. Bauer. *Minimal-footprint Middleware for the Creation of Qualified Signatures. International Conference on Web Information Systems and Technologies(WEBIST 2010).* Apr. 2010, pp. 64-69.

[23] https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

[24] www.ejbca.org/

[25] H. Kharche and D. S. Chouhan. Building Trust In Cloud Using Public Key Infrastructure -A step towards cloud trust. *International Journal of Advanced Computer Science and Applications*. Vol. 3, no. 3, Mar. 2012, pp. 26-31.

[26] J. Brown and P. Robinson. PKI Reborn in the Cloud. *Conference slides, RSA Conference Europe.* Oct. 2011, http://365.rsaconference.com/docs/DOC-3037 [retrieved: September 2015].

[27] https://nss-crypto.org/

[28] https://esign.cdac.in

[29] https://en.wikipedia.org/wiki/Representational_state_transfer