International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

e-Sign - An Online Digital Service: Evolving Trends & use Cases

Santosh K Pandey
Government of India
Ministry of Electronics and IT
New Delhi, India

Kavita Bhatia
Government of India
Ministry of Electronics and IT
New Delhi, India

Jahnavi Bodhankar
C-DAC
Ganesh Khind,
Pune, India

***Abstract*–Digital Signatures based on asymmetric crypto systems have been recognized as legally acceptable form of signing under the Information Technology Act, 2000. An electronic document signed using digital signature has the same acceptance as a handwritten signature. Cryptographic tokens are a widely used method for issuing Digital Signatures. However, issuance of a token requires various modes of verification based on identity and address proofs and the scheme is not scalable to billion people. For mass adoption of Digital Signature Certificate (DSC), a simple online service is desirable that allows one to have the ability to sign a document with ease. With that in consideration, an online scheme that uses the Electronic Know Your Customer (e-KYC) mechanisms from Aadhaar and provides the trust on documents in the form of digital signatures, eSign, is enabled by the Government of India since 2015. Various benefits that eSign provides include convenience and ease of operations to the signer, streamlined processes and reduction in the costs of operations largely associated with handling and storage of paper. Since the inception, eSign technology has been adopted by various sectors including e-Governance and Finance. Many more sectors are seen as potential use case for the technology.**

Keywords – PKI, Online Digital Signature, eSign, Token, DSC

I. INTRODUCTION

Digital Signatures are synonymous to hand written signature or a stamped seal. They provide a mathematical framework for assuring authenticity and integrity of a message, software or a digital document. The content to be signed is converted to Digital Fingerprint by hashing mechanism. Hash is then signed by a secret number known as Private Key to create the signature. A number known to everyone as Public key is used to verify the signature. Public key is distributed using Certificate that establishes an identity to the key. Certificate is to be issued from a trusted party. Thus, Cryptography hash function, Asymmetric Cryptography and Public Key Infrastructure provide the necessary building blocks for recognized and acceptable usage of Digital Signatures [1].

Cryptographic hash function is used to map digital content of arbitrary size to a fixed length string. It is a one way process with the characteristics of infeasibility to generate a message from its hash, difficulty to find another message with same hash and non-occurrence of same hash for two given different messages. It is a widely used method in Digital Signatures and Hash Based Message Authentication Code (HMAC) creation.

Public Key Cryptography employs asymmetric keys for the purpose of encryption and decryption. The keys exist in a pair known as Private-Public key and are mathematically related. RSA and ECDSA are common examples of Asymmetric Key. The key used to encrypt a text is different from the one used to decrypt. Digital signature use Private Key for signing purpose and Public key is used for verification of the signature. Strength of Public Key Cryptography lies in computational impracticality in deducing Private Key from Public Key and Security lies in protecting Private Key. Computational complexity limits the usage for short messages for example, data only as large as RSA key length can be encrypted using RSA key.

Public Key Infrastructure defines the comprehensive system required to manage digital signature certificates and public key infrastructure. The ecosystem recognizes Certifying Authority (CA) as a trusted party to verify the identity of a person/organization requesting for certificate, issue certificate, revoke the certificate and maintain certificate database. Increasing usage of Digital Media for data exchange has necessitated adoption of mechanisms to exchange information in a safe way. PKI system has been evolved and adopted by various countries over the last few years.

Some of the salient features of digital signature are:

- **Non-repudiation**: Digital signature is done using the unique key of the signer and thus ensures that the signer cannot deny later regarding signing the information.
- **Integrity**: Cryptographic message digest provides unique thumbprint of the data and provides an assurance of the data integrity during transmission.
- **Authenticity**: Digital signatures are unique to the key used for signing and the ownership of key is established based on the certificate issued by a trusted authority. Thus digital signatures provide a unique mechanism of authenticating the source of information.

II. GLOBAL SCENEARIO in PKI

In 2013, National Root Certification Authority of Thailand (NRCA) was established with the authorization for sub-CA issuance and compliance to international standards. Electronic Transactions Act B.E. 2544 (2002)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

and amended in 2008 recognized legality of digital signature in ecosystem of Thailand. Both Public and Private Sector CAs are recognized under the root CA. NRCA has also participated in interoperability tests among CAs of ASEAN member countries. E-mail security and e-Passport applications are most widely used in ASEAN [2].

Korea PKI system has two root CA authorities: National Root CA (KISA) and Government Root CA (GCMA). KISA was established in 1999 under Electronic Signature Act and issues certificate to Individual and Company based on SEED/AES algorithm. GCMA was established in 2001 in pursuant to E-Government Act and issues signature to Public Servants based on propriety algorithm. In order to achieve smooth operation among the two CAs, cross-certification based on Certificate Trust List has been defined [3].

III. INDIAN SCENEARION IN PKI

Indian IT Act 2000, 2006 provides legal sanctity to digital signatures considering them at par with handwritten signatures. Indian PKI follows a three-level hierarchy namely root CA as Controller of Certifying Authority (CCA), CAs with authorization from CCA for issuing certificates and Users. The Root Certifying Authority of India (RCAI) established under section 18(b) of the IT Act has the authority to digitally sign the public keys of CAs in the country and is operated as per the standards laid down under the Act. The root certificate is a self-signed certificate and is based on the ITU-T X.509 standard [4]. All certificates below the root certificate inherit the trustworthiness of the root certificate. The license issued to a CA is digitally signed by the CCA. The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country. CCA also empanels auditors for auditing infrastructure of CAs [5][6].

There are no CAs lower to the level of a CA and CAs can issue certain categories of certificates based on their authorization by CCA. CAs are required to maintain Certification Practice Statement(CPS) which is a statement of the practices a certification authority employs in issuing and managing certificates. Based on the CPS, CAs are required to change their key pair every 3-5 years. Currently length of CA key is RSA 2048 bits [5][6].

Today, in India most of the applications or forms submitted by a citizen require physical signature of the citizen. A digital signature takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." In the traditional Digital Signature system, an individual is responsible for applying for a crypto token and has to submit the identification proof and address proof.On the basis of the submitted documents the individual is provided the crypto token. The class of certificates includes class1, class2 and class3 etc. This traditional process is very time consuming and not feasible for mass adoption of Digital Signature Certificate (DSC) .With that in consideration, an online scheme that uses the Electronic Know Your Customer (e-KYC) mechanisms from Aadhaar and provides the trust on documents in the form of digital signatures, eSign, is enabled by the Government of India.

IV. ESIGN APPROACH

In the traditional Digital Signature system, an individual is responsible for applying for a Digital Signature Certificate to a CA for key pair generation and for safe custody of the keys. Issuance of certificate requires verification of Proof of Identity (PoI) and Proof of Address (PoA) beside other necessary information. The Certifying Authorities issue Digital Signature Certificate (DSC) to individuals after verification of identifications. Such Digital Signature Certificates are valid for a fixed duration, normally two to three years. The current scheme essentially has two drawbacks – scalability of digital signature service and security of the private key.

The Government has introduced Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 in which the technique known as "e-authentication technique using Aadhaar e-KYC services" has been introduced to eliminate stumbling block in the widespread usage of Digital Signature. This service is termed as "eSign Service". The service can be offered by Trusted Third Parties (TTP) or eSign Service Provider (ESP). Currently only licensed Certifying Authorities (CAs) can operate as ESP [7][14]. This mandates that the authentication issued by CCA must be followed for operating as ESP. These e-authentication guidelines are made available by CCA [11].

eSign is an online service that can be integrated within various service delivery applications via an open API to facilitate digitally signing a document by an Aadhaar holder. It is designed for applying Digital Signature using authentication of signer through Aadhaar authentication and e-KYC service. The various benefits that eSign provides include convenience and ease of operations to the signer, streamlined processes and reduction in the costs of operations largely associated with handling and storage of paper.

eSign leverages the e-KYC service of Aadhaar [8]-[10] for authenticating a signer. In the process, signer performs Aadhaar authentication using One Time Password (OTP) or Biometric data and authorizes UIDAI on successful authentication to provide demographic details along with photograph to eSign Service Provider only for the purpose of eSign. The details of the signer are used for generating certificate. The real-time e-KYC service makes it possible for service providers to provide instant service delivery to residents, which otherwise would have taken a few days for activation based on the verification of KYC documents, digitization, etc.

Once the signer is authenticated using Aadhaar service, a unique key pair is generated on behalf of the signer on a backend server, signing is carried on the hash of the document using RSA 2048/ECC 256 key and Certificate Signing Request (CSR) is generated for the eSign CA. eSign CA issues DSC for the signer. The key pair is deleted after one time usage. eSign CA can offer two classes of certificates: Aadhaar-e-KYC–OTP and Aadhaar-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

e-KYC–BIO based on the authentication mechanism used for authenticating a document signer.

V. STAKEHOLDERS AND THEIR ROLES

In the eSign workflow [7], [11]-[13], following are the main entities -

- *ASP – Application Service Provider*: ASP must ensure the security of the application as per the procedures defined by Controller of Certifying Authority (CCA) and Indian Computer Emergency Response Team (ICERT). ASP facilitates and provide necessary Interface/Application and infrastructure to an applicant for eSign. ASP is also required to sign contract and integrate Application with ESP to use eSign service.
- *ESP– eSign Service Provider*. ESP provides eSign service to the document signer by facilitating subscriber's key-pair generation, storing of key pairs on Hardware Security Module (HSM) and creation of digital signature. ESP is required to be a registered KYC User Agency (KUA) with UIDAI. As is necessary under the guidelines of CCA.
- *UIDAI – Aadhaar Authentication and e-KYC interface*: UIDAI provides unique identity to residents as per the authority established by Government of India for that purpose and runs the e-KYC authentication service for the registered KYC User Agency (KUA).
- *Document Signer*: Document Signer represents himself/herself for signing the document under the legal framework. The document signer shall also be the 'resident' holding the Aadhaar number and should have a registered mobile number with Aadhaar. For the purposes of DSC by the CA, the document signer shall also be the 'applicant/subscriber for digital certificate', under the scope of IT Act and provides the correct Aadhaar Number for eSign and will not impersonate anyone else.
- *CA - Certifying Authority*: CA is licensed by the CCA for issuance of Digital Signature Certificate and carries out allied CA operations such as maintenance of CRL etc. As is necessary under the guidelines of CCA, an eSign service provider must also be a CA.

The request for signing a document is given by the ASP to ESP. ESP uses the service of UIDAI for authenticating the document signer through its e-KYC mechanism. Upon successful authentication, it generates a key pair, computes the digital signature using the hash provided and returns to ASP the digital signature and digital signature certificate (DSC).

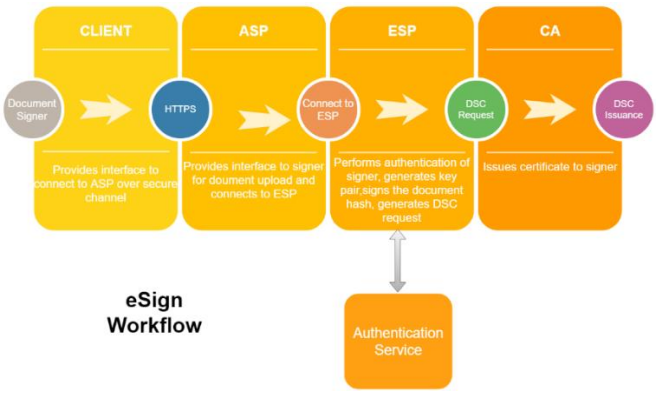

Figure 1: eSign Workflow

VI. ADVANTAGES OF ESIGN

eSign as an online Digital Signing service offers various advantages including:

- Saves Time: Use of eSign saves the time and can be easily accessed if needed at the remote location.
- Legally Recognized: The electronic signature is legally recognized by the Government of India.
- Managed By Licensed CAs: Only Certifying Authorities (CAs) issues Digital Signature Certificates (DSC) only after electronic authentication of user.
- Eco Friendly: eSign is a great initiative to go paperless and saves the paper and helps the business to sustain in the industry

VII. COMPARISION WITH SIMILAR INITIATIVES

Electronic Signatures are widely used in European countries. Three types of electronic signatures are recognized: Simple, Advanced (AdES) and Qualified (QES). Simple electronic signature is defined as data logically attached to other data in electronic form, such as writing name under an email. AdES is uniquely linked to and is capable of identifying signatory, provides signatory the control and is also linked to the document to detect incremental changes. QES is an advanced electronic signature created by a qualified signatory device such as smart card and is based on certificate issued by a trusted authority. Issuance and maintenance of Smart cards/USB Tokens are seen as cumbersome and expensive solutions [16].

To overcome the limitations, European Union (EU) Electronic Identification and Trust Services (eIDAS) regulations have recognized usage of server-held signing keys in a secure manner, thereby eliminating the management of keys by the signer in physical form and provisioning remote signing facility. Hardware Secure Modules (HSMs) are the devices used for managing server side keys. This however requires efforts to deploy and high cost maintenance for the service providers. With this in view, cloud based HSMs have evolved as the solution for mitigating the high costs involved in remote signing. For remote signing, a unique key is generated for each user and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

signature creation requires multi-factor authentication and key activation to ensure the security of the transaction.

Today various cloud platforms like Amazon and Microsoft Azure offers cloud HSMs as service. The signing keys can be generated and stored in the Azure or Amazon Key Vault HSMs.

The architecture of eSign has various similarities and dissimilarities to remote signing service used in EU. Both the methods support server end key generation and key usage. However, in eSign framework, a unique user key is created for every transaction, is used for single signing purpose and then the key pair is deleted. eSign utilizes e-KYC service of UIDAI for signer authentication. Remote signing entrusts e-KYC applications such as 'Belgian Mobile ID' compliant with eIDAS for authenticating signer during signature activation.

VIII. RECENT DEVELOPMENTS

Currently eSign utilizes online mechanism for authenticating a signer in real time. Recently, UIDAI has provisioned Offline Aadhaar e-KYC mechanisms usingdigitally signed XML [17]. An Aadhaar holder can generate his/her digitally signed Aadhaar details by accessing UIDAI resident portal. The details shall include mandatory and optional fields including Name, Address, Gender, DOB, Registered Phone Number (hashed), Registered Email Address (hashed) and Photograph. Digital signature of UIDAI on the data provides authenticity and integrity of the information. The data is downloaded as a zip file with share code. This file can be shared to any service provider as a proof of identity. The service provider is required to have the mechanism for verifying the digital signature on the file and use the credentials.

As a way forward, this new offline e-KYC mechanism shall be utilized for Identity and Address Verification by eSign Service Providers.

IX. USE CASE, CHALLENGES AND NEW OPPORTUNITIES

A. Use Cases

Presently, C-DAC offers its eSign service, named e-Hastakshar [14][15], to Aadhaar holders with registered mobile numbers using Aadhaar based e-KYC services to authenticate the document signer. A number of agencies are leveraging eHastakshar services in various citizen centric services and work flow based applications in Government and Private domains using authentication services of UIDAI such as

- Financial Sector
- Government agencies for internal office uses
- Legal Document Signing
- Direct Benefit Transfer
- Self-Attestation of documents
- GST Enrolment
- Citizen centric services

eSign is also being integrated in large scale applications such as Indian Payment Postal Bank for Bank Opening Form, Employee's Provident Fund Organization (EPFO) for Employee Registration/Employer Registration/KYC uploaded by employer/Transfer cases attestation by employers/e-Nomination/ Online request for change in Name/ DOB/Gender and Election Commission of India (ECI).

In the past 4 years' experience, we have analyzed that online Digital Signature method has been widely adopted in Financial, e-Governance, Administrative areas and Work-flow based applications. The ease of signing has enabled paperless Bank Accounts Opening, eMandates filing, Rent Agreement Registration, Home Loan Approval, Issuance of Birth/Death certificates, eOffice and Self-Attestation. The advent of Mobile applications providing services on-a-click, Digital India Initiative of Government of India for adoption of Digital services across the country/sectors, large user base in the above applications and desire to provide seamless services to the customers must have influenced early adoption of technology in these domains.

More than 9.5 core signatures have been issued in India till date. Integration of eSign in above mentioned applications has enabled paperless systems to function and help in saving time and paper.

B. Challenges

Despite availability of such a convenient, secured and time saving methodology of digital signing since a long time, following are the reasons that seem to deter its mass adoption:

- Lack of awareness: A digital signature has the same function as that of a handwritten signature. Some of its salient features are non-repudiation, integrity and authenticity. The Information Technology Act 2000 provides the required legal sanctity to digital signatures based on asymmetric crypto systems [14]. There is however a lack of awareness regarding this concept it seems, as despite availability of such a convenient and easy tool, most of the business establishments as also, Government departments still prefer manually signed documents and stamp paper based agreements while they have moved on to IT based solutions for their other day-to-day operations.
- Scalability: eSign requires a unique key pair generation for each transaction. Performance limitation of eSign system depends on the key generation speed as it is a non-deterministic process in nature. Impedance on scale cloud based HSM architecture could be a suitable solution in large scale applications, may to be evaluated.

C. New Opportunities

India has a huge market for eSign that remains largely unexplored owing to various reasons. BFSI (Banking, Financial Services, and Insurance) including Credit Card Service providers, hotel industry, health service industry including hospitals, eGov Service providers of all state

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 01, January-2020

governments, etc. are some of the most significant ones that can be immediately targeted.

Education field including schools/colleges can reduce the resources, cost and time required to issue various certificates by using online digital signing facility. Traditional system of document exchange includes scanning, faxing and posting. Usage of eSign can help reduce the cost and errors of the customary system by seamless use of online facility.

Online availability of medicines requires provision of scanned prescription by the patients. This puts in risk the authenticity of the prescription. eSign can provide a solution here, wherein digitally signed prescriptions may be accepted on portals to provide the necessary authenticity of the data.

X. CONCLUSION AND FUTURE WORK

e-Sign framework has evolved as part of Government of India's Digital India Initiative. The e-Sign service makes governance, national programs and information simpler for India's citizens. By using e-Sign in an application, we can save time and make life simpler for the citizens. Past 3 years' experience has shown a good acceptance of the technology in the domains viz. legal, e-governance, financial and administration.

Offline e-KYC mechanism provides a way forward to integration of new authentication methods in eSign Architecture. The technology scope needs to be expanded in various other fields like healthcare and education. Taking in account the increasing need and demand of the eSign, we should look forward for the approach like cloud based HSM, which is highly scalable, cost effective, time saving and secured.

Disclaimer: *'The views expressed in this article are the views of the authors in their personal capacities, which do not represent the views of MeitY/C-DAC'.*

REFERENCES

[1] SlideShare, 23-Dec-2016,An overview of Digital Signatures, PKI. [Online]. Available: https://www.slideshare.net/RishiPathak1/digital-signature-esign-overview. [Accessed: 10-Dec-2019]

[2] India PKI Forum, "n.d.", 'PKI Development in Thailand'. [Online]. Available: http://www.indiapki.org/presentation/PKI%20Development%20in%20Thailand%20-%20by%20Dr_Chaichana.pdf. [Accessed: 10-Dec-2019]

[3] SlideShare, 17-Apr-2015, 'PKI In Korea'. [Online]. Available: https://www.slideshare.net/meruvian/pki-in-korea. [Accessed: 10-Dec-2019]

[4] Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T X.509 (10/2016), October 2016

[5] Controller of Certifying Authority, "n.d",'About CCA'. [Online]. Available: http://www.cca.gov.in/cca/?q=about.html. [Accessed: 10-Dec-2019]

[6] Vikas Rattan, Er. Mirtunjay Sinha, Vikram Bali and Rajkumar Singh Rathore., "E-Commerce Security using PKI approach", International Journal on Computer Science and Engineering, Vol. 02, No. 05, pp 1439-1444, 2010

[7] Controller of Certifying Authority, "n.d", "eSign". [Online]. Available:http://www.cca.gov.in/cca/?q=eSign.html. [Accessed: 10-Dec-2019]

[8] Unique Identification Authority of India, March 2018,'Aadhaar Authentication API Specification - Version 2.5'. [Online]. Available:https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf.[Accessed: 10-Dec-2018]

[9] Unique Identification Authority of India, March 2018, 'Aadhaare-KYC 2.5 Specification – Version 2.5'.[Online]. Available:https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_5.pdf.[Accessed: 10-Dec-2019]

[10] Unique Identification Authority of India, March 2018,'Aadhaar OTP 2.5 Specification – Version 2.5.[Online]. Available:https://uidai.gov.in/images/resource/aadhaar_otp_request_api_2_5.pdf. [Accessed: 10-Dec-2019]

[11] Controller of Certifying Authority, June 2018, 'e-authentication guidelines for eSign- Online Electronic Signature Service - Version 1.4'. [Online]. Available:http://www.cca.gov.in/cca/sites/default/files/files/ESIGN/CCA-EAUTH.pdf. [Accessed: 10-Dec-2019]

[12] Controller of Certifying Authority, April 2017, 'CCA's Draft ASP On-boarding guidebook –Version 1.2'. [Online]. Available:http://www.cca.gov.in/cca/sites/default/files/files/ESIGN/CCA-ASP.pdf. [Accessed: 10-Dec-2019]

[13] Controller of Certifying Authority , June 2018, 'Interoperability Guidelines for Digital SignatureCertificates issued under Information Technology Act – Version 3.5'. [Online]. Available: http://www.cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IOG.pdf. [Accessed: 10-Dec-2019]

[14] Center for Development of Advanced Computing, 2015, 'e-Hastakshar: C-DAC's On-line Digital Signing Service'. [Online]. Available: http://esign.cdac.in/. . [Accessed: 10-Dec-2019]

[15] Center for Development of Advanced Computing, 2015, 'C-DAC Certification Practice Statement'. [Online]. Available: https://esign.cdac.in/ca/CPS/CPS.pdf. [Accessed: 10-Dec-2019]

[16] CEF Digital, "n.d", "eSignature". [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=46992760. [Accessed: 12-Dec-2019]

[17] Unique Identification Authority of India, 2018, 'Aadhaar Paperless Offline e-kyc Verification'. [Online]. Available: https://uidai.gov.in/authentication/authentication-devices-documents/aadhaar-paperless-offline-e-kyc-verification.html. [Accessed: 10-Dec-2019]

[18] Johnson, D., Menezes, A. & Vanstone, S., "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Journal of Information Security, Volume 1, Issue 1, pp 36-63, August 2001https://doi.org/10.1007/s102070100002

[19] Dindayal Mahto and Dilip Kumar Yadav, "RSA and ECC: A Comparative Analysis", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19, pp. 9053-9061, (2017)

[20] VincentLozupone, "Analyze encryption and public key infrastructure (PKI)", International Journal of Information Management, Volume 38, Issue 1, pp 42-44, February 2018

[21] Vijay Jain, Ranjan Kumar and Zia Saquib, "An Approach towards Digital Signatures for e-Governance in India", EGOSE '15 Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia, pp 82-88, November 2015

[22] Controller of Certifying Authority, "eSign Gazette Notification". [Online]. Available:http://www.cca.gov.in/cca/?q=eSign_gazette_notification.html. [Accessed: 10-Dec-2019]