Project profile for eAsia Awards 2015

Country/Economy: India

Date: 31-Aug-2015

Project Title: eSign

Organization: eMudhra Limited

Category:
Bridging Digital Divide

Project Leader: Vijay Kumar M

Job title: SVP & Head of Technology

Phone Number: +91-80-42275351

Email Address: eservices@emudhra.com

Contact Person: Vijay Kumar M

Mailing Address:
eMudhra Limited, Sai Arcade, 3rd Floor, No.56, Outer Ring Road, Bangalore, Karnataka, India. Postal Code: 560103

Phone Number: +91-7760092828

Fax:

Email address: vijay@emudhra.com

URL: www.e-mudhra.com / www.eservices.emudhra.com

This form is completed and submitted by:
Vijay Kumar M
Signature:

Vijay

Project Title	eSign

Project Leader Name	Vijay Kumar M
Organization/Company	eMudhra Limited
Nominated by	Mr. A. K. Sinha

Abstract

eSign project enables Indian residents to digitally sign any document using Aadhaar. This online electronic signature service can be integrated with service delivery applications via an open API to facilitate an Aadhaar holder to digitally sign a document. Using authentication of the Aadhaar holder through Aadhaar e-KYC service, online electronic signature service is facilitated.

This project is an incentive for digitization aspirants, as it gives legal assurance, non-repudiation and authenticity of the transaction just like a physical counterpart does. This paves way for more and more peopled to easily come to digital world and transact securely; thus bridging digital divide.

Executive Summary

Background:

Aadhaar is a national project of Government of India, which allocates an Unique Identification number to Indian residents. As on date, more than 90 Crore (900 million) residents have been allocated with Aadhaar, which contains the resident identity, address, biometric information, etc. The details are authentic and facilitated through national agency.

eMudhra is a certifying authority in India regulated under Indian Information Technology Act, by Controller of Certifying Authorities (CCA), Ministry of IT, Government of India. Since inceptions, eMudhra is facilitating Digital Signature Certificates to more than 2 million subscribers in conventional mode. This includes physical application from subscriber, verification by CA, issuance of certificate to a FIPS certified token, etc.

The above conventional mode has its one hassles in terms of procurement and retention of certificate in the subscriber custody. This is more challenging for one-time signers who has to sign just single document or tax return in a year.

Electronic Signature Scheme:

Indian Information Technology act defines electronic signature. But, it was just covering conventional Digital Signature Certificate that can be procured physically and stored in USB crypto token. Government of India amended the act and introduced second schedule with a new concept of electronic signature. This permits the subscribers to digitally sign using online authentication mechanism. This relies on electronic KYC process of Aadhaar system to validate the Identity proof and Address proof of the applicant.

eMudhra eSign Service:

Even though the regulation was put in place on January - 2015, the system had to be prototyped, architected and converted to technical implementation. eMudhra took this as a challenge and re-engineered its systems to make a successful launch.

e-Sign facilitates electronically (digitally) signing a document by an Aadhaar holder using an Online Service. While authentication of the signer is carried out using eKYC of Aadhaar, the signature on the document is carried out on a backend server, which is the e-Sign provider. The service can be run by a trusted third party service provider, like Certifying Authority. To begin with the trusted third party service shall be offered only by Certifying Authorities. The eSign is an integrated service that facilitates issuing a Signature Certificate and performing Signing of requested data by authenticating AADHAAR holder. The eSign Service shall be implemented in line with e-authentication guidelines issued by Controller. The certificate issued through eSign service will have a limited validity period and is only for one-time signing of requested data, in a single session.

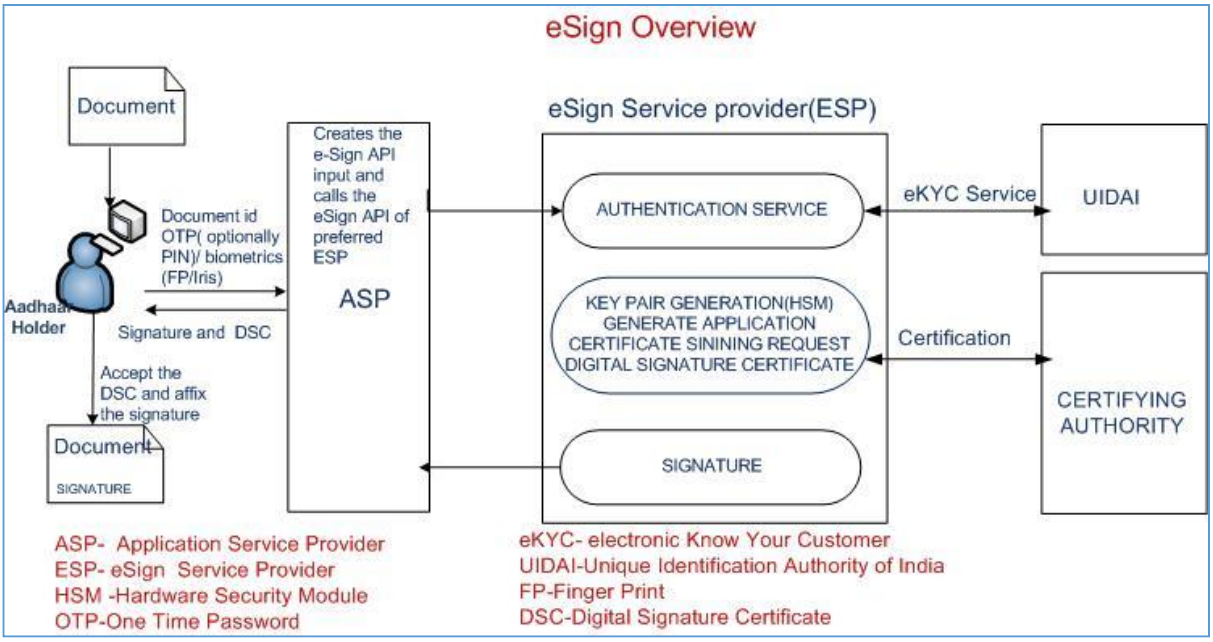
Being the first empanelled eSign Service Provider on June-2015, eMudhra now serves the national Digital India project “Digital Locker” with eSign facility. This enables Indian resident to sign any document online in a matter of seconds.

Project Content

Project scope

The scope of the project is to engineer the concept of electronic signature, with a standard REST API, and make the technical implementation. The API should be able to serve maximum concurrency with speedy response.

Below diagram illustrates the overall scope of the project.


eSign Overview
Document
Document id
OTP(optionally PIN)/ biometrics (FP/Iris)
Aadhaar Holder
Signature and DSC
Accept the DSC and affix the signature
Document
SIGNATURE
Creates the e-Sign API input and calls the eSign API of preferred ESP
ASP
eSign Service provider(ESP)
AUTHENTICATION SERVICE
KEY PAIR GENERATION(HSM) GENERATE APPLICATION CERTIFICATE SININING REQUEST DIGITAL SIGNATURE CERTIFICATE
SIGNATURE
eKYC Service
UIDAI
Certification
CERTIFYING AUTHORITY
ASP- Application Service Provider
ESP- eSign Service Provider
HSM -Hardware Security Module
OTP-One Time Password
eKYC- electronic Know Your Customer
UIDAI-Unique Identification Authority of India
FP-Finger Print
DSC-Digital Signature Certificate

Terminologies

Application Service Provider (ASP): An organization or an entity using eSign service as part of their application to electronically sign the content. Examples include Government Departments, Banks and other public or private organizations. ASP may contact the ESP (eSign Service Provider) directly to avail the service within its framework.

End-User: An Individual using the application of ASP and represents himself/herself for signing the document under the legal framework. For the purposes of KYC with UIDAI, the end-user shall also be the ‘resident’ holding the AADHAAR number. For the purposes of DSC by the CA, the end-user shall also be the ‘applicant/subscriber for digital certificate’, under the scope of IT Act.

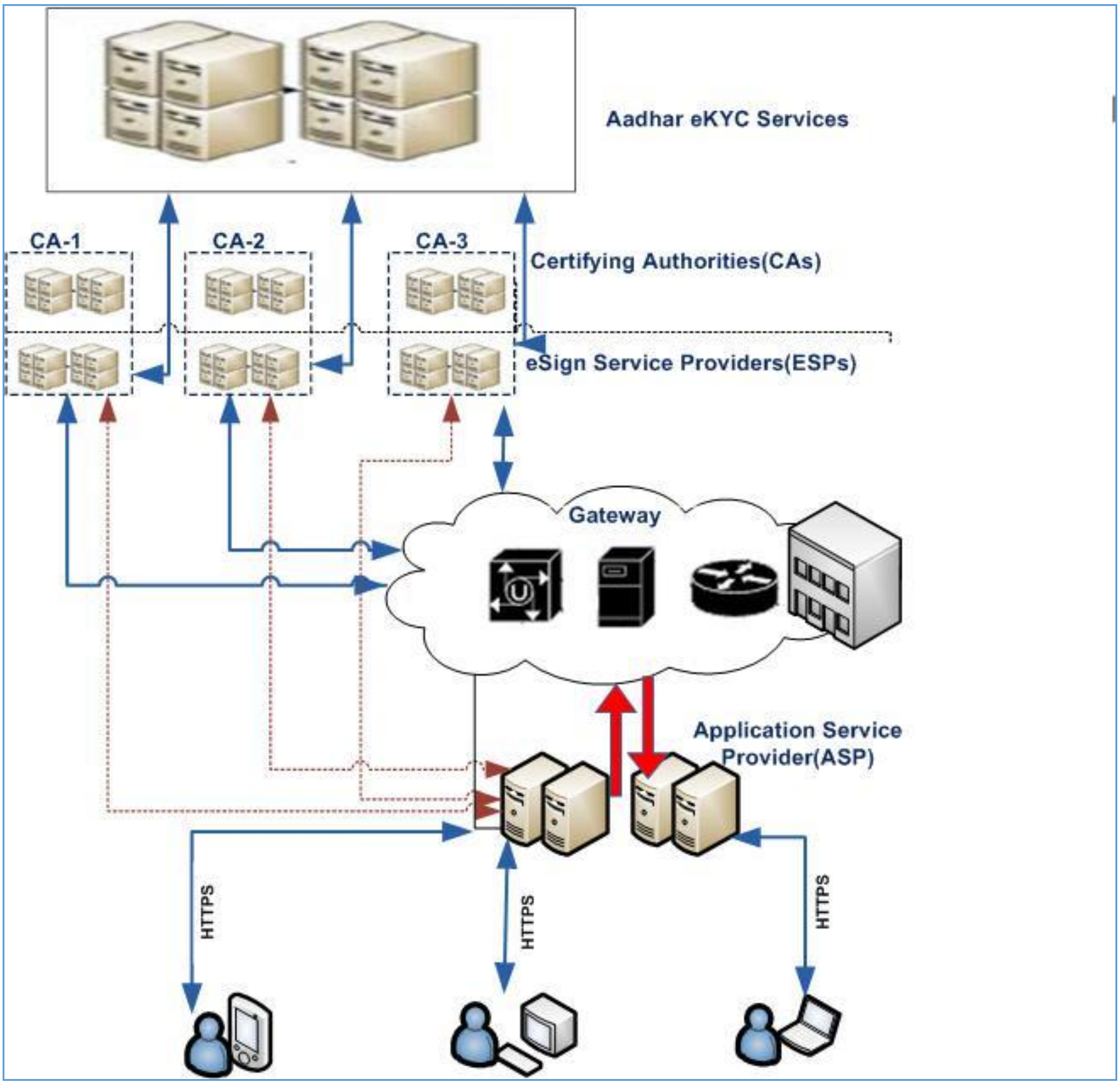
eSign Service Provider (ESP): eMudhra Limited. An organization or an entity providing eSign service. ESP is a "Trusted Third Party", as per the definitions of Second Schedule of Information Technology Act. ESP must be a registered KYC User Agency (KUA) with UIDAI. ESP will facilitate subscriber's key pair-generation, storing of key pairs on hardware security module and creation of digital signature. ESP can be a Licensed Certifying Authority (CA), by themselves, or must be having an arrangement / integration with a CA for the purpose of obtaining Signature Certificate for the generated Key-pair.

Certifying Authority (CA): eMudhra Limited. An organization or an entity licensed under CCA for issuance of Digital Certificate and carrying out allied CA operations.

UIDAI: An authority established by Government of India to provide unique identity to all Indian residents. It also runs the eKYC authentication service for the registered KYC User Agency (KUA).

eSign framework

Following Diagram depicts the framework of eSign service.


Aadhar eKYC Services
CA-1
CA-2
CA-3
Certifying Authorities(CAs)
eSign Service Providers(ESPs)
Gateway
Application Service Provider(ASP)
HTTPS
HTTPS
HTTPS

Goals and objectives

The goal of the project is to achieve a technical solution to facilitate eSign API.

The objectives are as under:

1. Development of REST API to perform the operation in single session.
2. Facilitate concurrent incoming requests.
3. Generate end user Key Pair in HSM
4. Securely contact Certifying Authority System with an internal API.
5. Develop a new simplified CA System to facilitate high volume transactions
6. Connect to UIDAI (Aadhaar) server and perform eKYC
7. Perform signing of the input document.

8. Meet the compliances as defined in IT act and rules

Challenges

While the goal is to simplify the digital signing model with an one-time use key-pair, it has several operational and technical challenges.

1. Enrolment with government agency for Aadhaar eKYC.
2. Performing Biometric / OTP based eKYC of the end user.
3. Make external signing of document, based on document hash.
4. Build an Application Service Provider system to simulate the system.
5. Load testing the application, as successful transaction simulation is practically difficult.

Strategies

eMudhra strategized the overall goal to independent tasks, in order to discipline the timeline, keeping the integrated solution intact.

1. Choosing the right technology.
2. Setting up environments - develop, test, pre-production & production
3. Sizing the hardware requirements, Bandwidth and network constraints
4. External dependencies - Aadhaar integration, CA integration
5. Architecting the project, and solutions underneath
6. Develop, test & integrate
7. Allow external agencies to integrate live.
8. Audit requirement of regulator
9. Project - Go Live

The idea here is to first sequence the activities to be performed and then evolve the methodologies to achieve it.

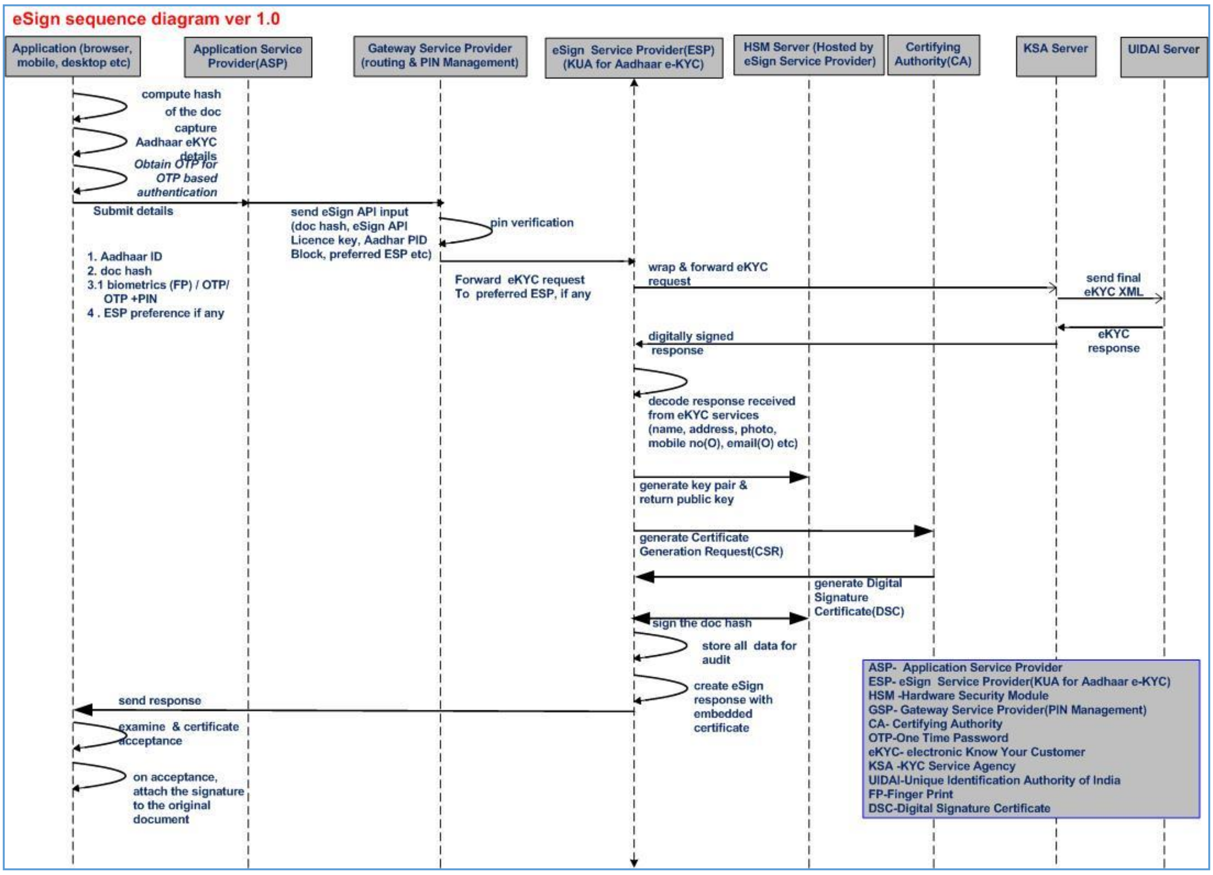
Methodology

The project required deep expertise in public key infrastructure (PKI) along with RSA. Along with, it was insufficient to have just the core knowledge to build a large project.

eMudhra derived a methodology to handle various aspects of the project independently. The team was carefully constructed towards optimum results. In fact, it required several research activities which was taken on top most priority.

The positive results of core research in sensitive areas added more power to the task force. Once the key areas are handled, the technical sequencing of the project was taken up.

Below diagram illustrates the technical sequencing process of overall project.


eSign sequence diagram ver 1.0
Application (browser, mobile, desktop etc)
Application Service Provider(ASP)
Gateway Service Provider (routing & PIN Management)
eSign Service Provider(ESP) (KUA for Aadhaar e-KYC)
HSM Server (Hosted by eSign Service Provider)
Certifying Authority(CA)
KSA Server
UIDAI Server
compute hash of the doc
capture Aadhaar eKYC details
Obtain OTP for OTP based authentication
Submit details
1. Aadhaar ID
2. doc hash
3.1 biometrics (FP) / OTP/ OTP +PIN
4 . ESP preference if any
send eSign API input (doc hash, eSign API Licence key, Aadhar PID Block, preferred ESP etc)
pin verification
Forward eKYC request To preferred ESP, if any
wrap & forward eKYC request
send final eKYC XML
eKYC response
digitally signed response
decode response received from eKYC services (name, address, photo, mobile no(O), email(O) etc)
generate key pair & return public key
generate Certificate Generation Request(CSR)
generate Digital Signature Certificate(DSC)
sign the doc hash
store all data for audit
create eSign response with embedded certificate
send response
examine & certificate acceptance
on acceptance, attach the signature to the original document
ASP- Application Service Provider
ESP- eSign Service Provider(KUA for Aadhaar e-KYC)
HSM -Hardware Security Module
GSP- Gateway Service Provider(PIN Management)
CA- Certifying Authority
OTP-One Time Password
eKYC- electronic Know Your Customer
KSA -KYC Service Agency
UIDAI-Unique Identification Authority of India
FP-Finger Print
DSC-Digital Signature Certificate

At this point of time, it was easy to stitch together the individual results and put it as per the architecture. The end result was witnessed with very less errors. After the certificate by Quality Assurance (QA) team, the entire project was then put up to pre-production environment.

By this time, all the external dependencies were addressed, and a few Application Service Providers (ASP) were ready to integrate. With a favourable response from ASP, eMudhra was able to successfully integrate eSign service with their applications. Thus, the end users using such application are facilitated with eSign.

Re-engineering

To achieve the project goal, eMudhra had to re-engineer several areas. Lot of time was put into initial research and re-engineering, before working on the main project. Some of the re-engineered tasks are as under:

1. New CA certificate system for eSign.
2. Signing of Document Hash (SHA 256), which should be a compatible RSA signature, verifiable against original document.
3. Detached PKCS#7 signature by signing the hash of the document.
4. Hardware remodelling to achieve the optimum result.

Standards

eMudhra adopted various standards towards the project, namely:

1. RFC compliance for digital signature.
2. eSign API standards of the regulator.
3. ISMS towards project development.

Economic benefits, achievements, and impacts

The project stands large in terms of government of India's Digital India vision. The project is renowned for its vision towards simplifying electronic transactions and documents, thus achieving a digital revolution. The paperless revolution is now being adopted by large banks, telecom providers, stock trading agencies, and several G2B, B2B, G2C and B2C projects. The project benefits Indian residents where they can now open a bank account, or apply for a government scheme, or get a telephone connection without physical paper. The secure, authentic, non-repudiated transactions ensures complete trust on the digital transaction / document.

The project has achieved a milestone as the first and only eSign provider integrated with Government of India's Digital Locker project. eSign was launched by honourable prime minister Mr. Narendra Modi on 02-July-2015.

With this, thousands of eSign transactions take place every day with the acceptability increasing across various organizations.

The project has made a national level impact with more and more agencies wanting to implement the service and go paper-free. This not only eases the end user, but also saves lot of operational and physical retention hassles to the organizations.

In today’s world, eSign easily makes it compatible to go digital through Mobile devices. eSign with OTP authentication has already been visualized as a use case for m-governance.

eMudhra has already demonstrated the concept at various organizations. Below are some of the use cases, where eSign is being adopted:

1. Application form of Banking, Telecom, etc
2. Government subsidy / pension claims
3. Office document workflow
4. Public to Government communications
5. Person to person document transaction
6. Stock / security contracts

eSign carries high credibility towards bridging the digital divide. It encourages people to adopt digital transactions, and be paper-free.

Next step on ward

eMudhra now aims at taking the project implementation to large segment of people. With an innovative free-transaction model, it is now easy for ASP to integrate eSign in their system.

This model is taken to several business organizations, from small to large. The project is focussed to integrate with electronic transaction software including banking, insurance, trade, e-commerce, government and many more.

Any Aadhaar Holder will be able to subscribe to eSign with a nominal fee and transact freely anywhere.

eMudhra has launched an “eSign PDF” utility which can be freely downloaded from website, and use it for signing any PDF document. This is expected to revolutionize, the way signed electronic transactions happen.

In a medium term, eSign is expected to achieve more user adoption and digitize several processes. The concept being closely examined by trade and industry, this also eases the digitization of regular paper transactions like Purchase Order, Invoices, Receipts, etc. On the other hand, the government regulators’ interest to adopt it for tax return filing, annual returns, etc will not only digitize those transactions, but also popularize the eSign adoption to a large set of people.

Resources

eMudhra’s approximate resource allocations are as under:

Resource	**Expense (in INR)**	**USD**
Manpower	75,00,000	$115385
Hardware	1,00,00,000	$153846
External Software	5,00,000	$7692
Networking and Bandwidth	10,00,000	$15385
Infrastructure	10,00,000	$15385
Administration	5,00,000	$7692
Total	**2,05,00,000**	$315385