



National Conference on Digital Signature & Public Key Infrastructure (PKI)

Use of eSign in e-Governance Services

Centre for e-Governance
Government of Karnataka

17th June, 2016



PKI in e-Governance – Current Scenario

G2C

- Citizen's interaction with department through G2C application:
 - Citizen fills up application forms through web based application of departments:
 - Example: for education and identity certificates , scholarship , pension , commercial tax, in transport department ,department of revenue, fisheries department etc
 - Takes a print out of the application
 - Physically signs the documents
 - Submit the documents to the government department

Process remains as cumbersome as before for citizens

G2G

- Digital certificates have been provided to limited government officials for digital signing of documents



PKI in Government – Current Scenario (CONTD.)

- Key department users of PKI in GoK
 - Treasury Department
 - 25,000 Drawing & Disbursement Officers (DDOs) uses Digital Signature for approvals / sanctions for uploading to the central processing system in Khajane II
 - e-Procurement
 - Citizen uses digital certificate to sign the financial quotes and it is encrypted
 - Tender Accepting Authority decrypts the financial bid
 - More than 65,000 tenders where floated through e-Procurement platform in FY 2015-16
 - More than 3 Lakhs registered user in e-Procurement Platform
 - Human Resource Management Systems (HRMS)
 - 21,000 Drawing & Disbursement Officers (DDOs) uses Digital Signature for approvals / sanctions for uploading to the central processing system in Khajane II



Use Case: Treasury - Khajane II

Khajane II - Google Chrome

https://10.25.1.23/KHAJANE/digigov.htm?actionFlag=doPopulateInboxForAdmin&elementId=10000064

Employee Registration For 1214947-P.MALATHI -

First Name: P.MALATHI
Employee name: HRMS: P.MALATHI
Gender: Female
Date of Joining: 18/06/1992

Last Name: -
Cadre: SECONDARY STAFF ASSISTANT
Gazetted / Non Gazetted: Non Gazetted

Map post to the Employee

Admin Department: FINANCE DEPARTMENT
Field Office: COMMERCIAL TAXES (APP)
Primary Post: STENOGRAPHER-1

Directorate Department: COMMERCIAL TAXES DEP
Cadre: SUPPORTING STAFF-C

Add Secondary Post

Admin Department: --Select--
Field Office: --Select--
Secondary Post: --Select--

Directorate Department: --Select--
Cadre: --Select--

Add

Upload R1 form (Certification Form) & R2 form (Certificate of Posting)

Attachment:

Note: Maximum 2MB Allowed (Only PDF, PPT, JPG, PNG are allowed)

File: [Choose File] No file chosen
Add Attachment

Description	File Name	Action
N/A	a.JPG	Remove / View

Scanned Employee Signature

Attachment:

Note: Maximum 2MB Allowed (Only PDF, PPT, JPG, PNG are allowed)

File: [Choose File] No file chosen
Add Attachment

Description	File Name	Action
N/A	a.JPG	Remove / View

Approve Return Reject Close

Copyright 2014. All rights reserved. Fields marked with * are mandatory. All amounts are in INR. All the dates are in DD/MM/YYYY format. Build Version: 3.9.6

12:10 24-06-2015

AADHAAR

Data to be signed



Use Case: e-Procurement

https://eproc.karnataka.gov.in/eprocurement/jsf/tender/sign_tender.seam?conversationId=98738&conversationIsLongRunning=true

PROCUREMENT PORTAL

Wednesday, 21 October 2015 18:31:59

Welcome Dr Rathan Kelkar, CEO CEG

My Profile Indent Management Tender Management Catalogue Management
Contract Management Auction Management Project Management

General Details

Tender Number : CEG/31/UID/2015
Description : Supply of Tablets and Single finger authentication device for Aadhaar project
Tender Category : SERVICES
Tender Evaluation Type : THREE_COVER
Tender Type : OPEN
Commercial Bid Type : ITEM_WISE

Tender Amount Details

Estimated Contract Value : 35000000

Sign and Send For Approval

Sign :*

Send To:* SRIVATSA KRISHNA - Chairman

Working

Close Send For Approval

Enter PIN

To log in to "RATHAN U KELKAR"

Enter PIN:



✓ Minimum PIN length 4 bytes
✓ Maximum PIN length 15 bytes

OK Cancel

Data + Financial Bid document to be signed



Use Case: HRMS

ORGANOGRAM

Department : KARNATAKA STATE POLICE

As Per Format2(Khajane)

Select	Sno	Post	Cadre	Department Name	Permanent	Temporary	Deputation	Getting Post Encadre From	Sending Post Encadre To	Permanent + Temporary	Getting Post Encadre From Count	Sending Post Encadre To Count	Permanent + Temporary Count
	1	Director General & Inspector General of Police, Bangalore	Director General & Inspector General of Police	KARNATAKA STATE POLICE	1	0	0						
	2	Annexure-1	Director General of Police	KARNATAKA STATE POLICE	2	0	2		0	1	3	0	1
	3	Lecturer	Lecturer	KARNATAKA STATE POLICE	5	0	0	5	0		5	0	
	4	Website Hacker	Website Hacker	KARNATAKA STATE POLICE	2	0	0	2	0	0	2	0	0
	5	Scientific Officer (Chemical Section)	Scientific Officer (Chemical Section)	KARNATAKA STATE POLICE	33	1	0	0	32	2	0	32	2
				KARNATAKA			0						

Data to be signed

Users fill these fields



Limitations – Current Scenario

- Handling of Dongle based Digital Certificates
 - Procurement & maintenance of dongles
- Security
 - Risk of misuse
- Initial & recurring Cost
- Periodic renewals
- Not a scalable solution
- Large number of business processes have not incorporated digital signing because of scalability, distribution and control issues.



New Paradigm: e-Sign

- e-Sign methodology will enable citizens to submit digitally signed web based application forms and documents on-line
 - No need for Digital Certificate dongle, thus achieving scalability
 - Paper less applications by citizens for education/identity certificates, scholarship ,pensions , commercial tax, in transport department, department of revenue etc.
- Can scale up to any level for Approvals & Sanctions within government
- Impersonation - Guarantees that the signature is from the person, whom it is supposed to be.
- Ease of signing by Residents/ government staff
 - Easy way for government officials for digitally signing any documents at any levels.
 - Paper less (or less paper) communication
 - Protects government/ enterprises from non-repudiation and legal sanctity.



e-Sign Interface in Web Application

Typical web page interface:

e-Procurement Portal

Tender Number :

EMD Paid : ☐ YES ☐ NO

TECHNICAL PROPOSAL

UPLOAD FILE :

XYZ.doc

FINANCIAL PROPOSAL

UPLOAD FILE :

abc.exlxs

TOTAL COST OF PROPOSAL :

Enveloped XML
Signature

E-Sign Pop up
Window



e-Sign Pop-up Window

e-Sign Popup Window

Please enter your Aadhaar Number

I hereby authorise ESP to

1. accessing my identity and address data through Aadhaar eKYC Services
2. Generate and submit the electronic DSC application form to CA.
3. create key pairs and submit of certificate Signing Request for DSC Generation

4. one time creation of signature for this document/information

I understand that the key pair will be deleted immediately after applying Signature

I Agree: Yes/No

Select Authentication Type

☒ One Time Password

☒ Biometric

Type One time password



e-Sign Response

“e-Sign is successful”

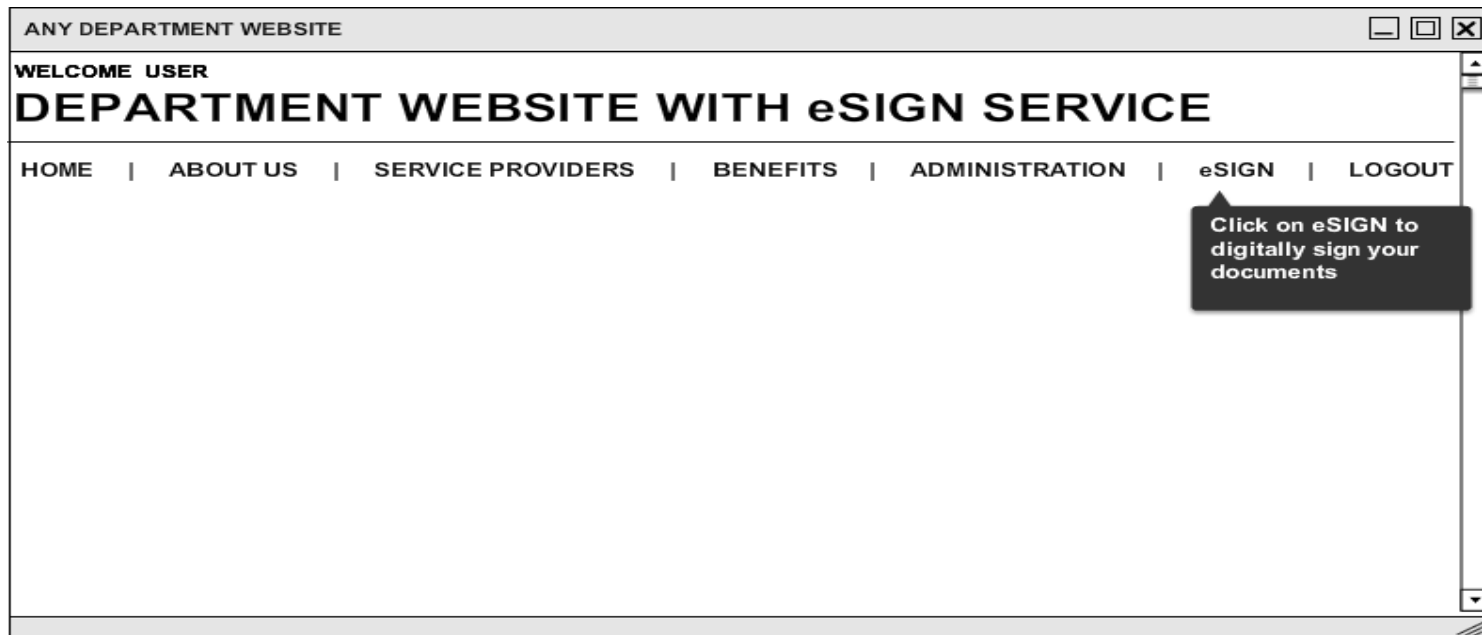
Your Transaction ID is <transaction ID>. Please use the transaction ID for future references.

Optional – May be suppressed



e-Sign in Stand-alone Mode

- Department can provide stand-alone tab & interface for the staff to digitally sign any document or **multiple documents** to:
 - Send it across to other person (thru email etc.)
 - Upload the digitally signed file in Digi-locker or any other website.





e-Sign in Stand-alone Mode (CONTD.)

Upload Document

Upload File(s) :

On click eSign section is displayed

eSign

Enter Your Aadhar Number :


I hereby authorise ESP to

1. accessing my identity and address data through Aadhaar eKYC Services
2. Generate and submit the electronic DSC application form to CA.
3. create key pairs and submit of certificate Signing Request for DSC Generation
4. one time creation of signature for this document/information

I understand that the key pair will be deleted

I AGREE : ☐ YES ☐ NO

Authentication type

BiMetric : 

eSign Response

"eSign Successfull"

Your Transaction Id is < Transaction ID >. Please use Transaction ID for future reference

Save the file :

After signing, document can be saved in the local system.



e-Sign by Resident in KRDH

Department staff or citizen, who do not have access to any web application but would like to e-sign any document through **Resident portal of KRDH (for resident)**.

KRDH → Resident → KRDH Services

Window Title

WELCOME USER

HOME | ADMINISTRATION | LOGOUT

Karnataka Resident Data Hub

AADHAAR

SELF MAPPING

AADHAAR INFORMATION

BENEFICIARY INFORMATION

KRDH Services

SERVICES

DIGILOCKER

eSIGN

RESIDENT DATA

USER HELP DESK

HELP DESK



e-Sign by Resident in KRDH (CONTD.)

Upload Document

Upload File(s) :

On click eSign section is displayed

eSign

Enter Your Aadhar Number :


I hereby authorise ESP to

1. accessing my identity and address data through Aadhaar eKYC Services
2. Generate and submit the electronic DSC application form to CA.
3. create key pairs and submit of certificate Signing Request for DSC Generation
4. one time creation of signature for this document/information

I understand that the key pair will be deleted

I AGREE : ☐ YES ☐ NO

Authentication type

BiMetric : 

eSign Response

"eSign Successfull"

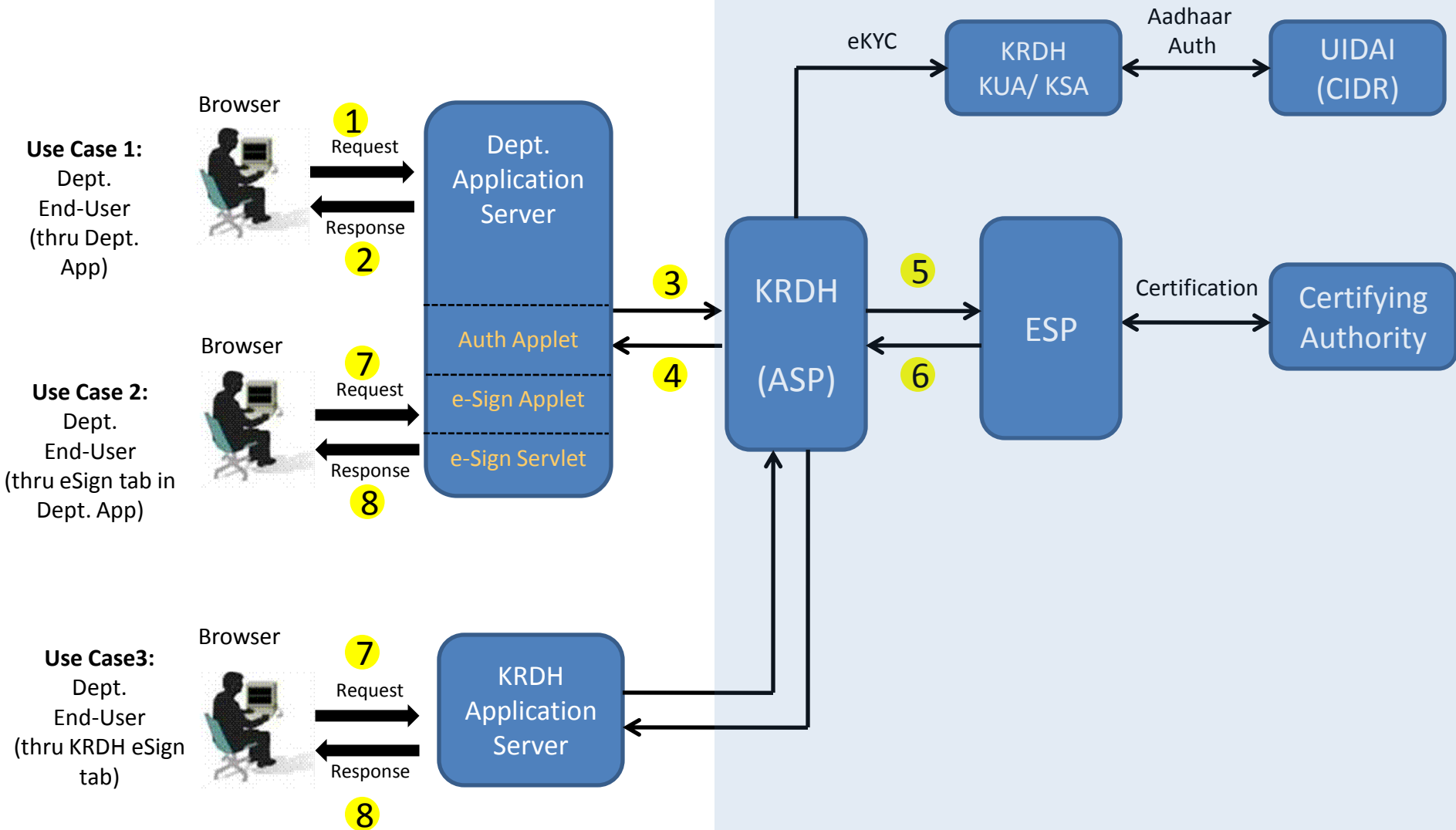
Your Transaction Id is < Transaction ID >. Please use Transaction ID for future reference

Save the file :

After signing, document can be saved in the local system.



KRDH e-Sign Architecture





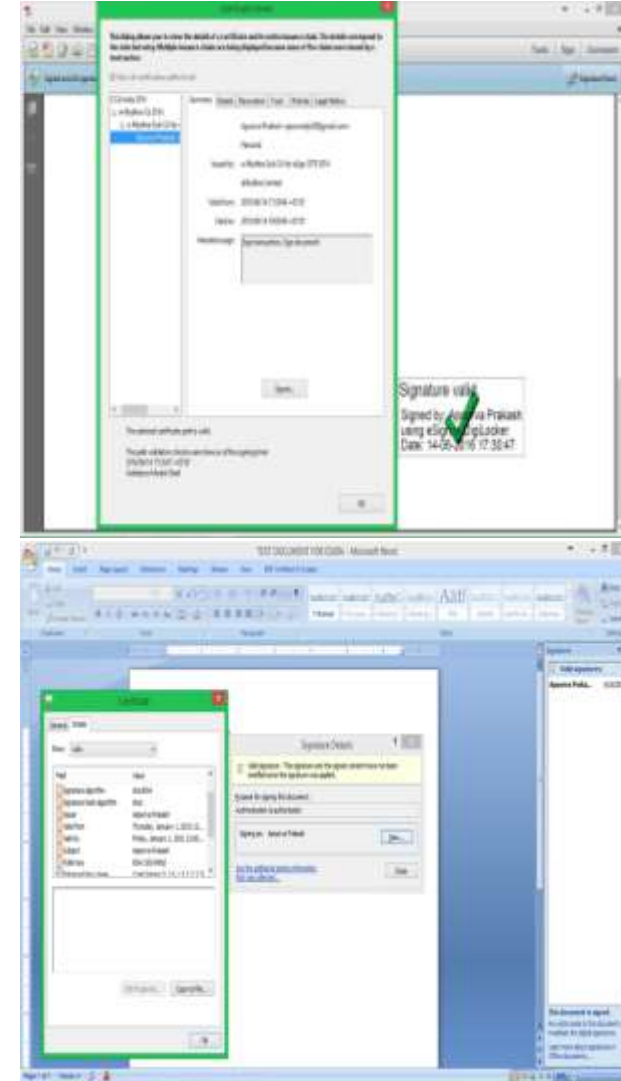
e-Sign Volume Estimation

- Digi-Locker - dependency on e-Sign
- Volume Estimation – **32 Cr** Transaction per year
 - 16 Cr e-Sign transactions per year are expected for departmental sanctioning/ approval process
 - 15 Cr e-Sign transactions per year are expected for Digi-locker document signing.
- Processing Capacity – **1.6 Lakhs** transactions per hour



Challenges & Issues

- MSOffice document Signing
 - Interactive MSWord signing vis-à-vis *.pdf* signing
- Multiple signature in a document
- Bulk Signing
- Same signature in the multiple pages
- Signature for server level communication
 - Equivalent of Document Signer
- Scaling up of IT Infrastructure for the entire eco-system





Food for thought

Sample Sale Deed



ABSOLUTE SALE DEED

This DEED OF ABSOLUTE SALE is made and executed at Bangalore, on this Second day of May, Two Thousand Sixteen (02/05/2016) BY AND BETWEEN -

(1) **Sri.JAI PRAKASH,** (PAN No.APQPP8753G)
S/o. Late Mr.D.Anthony & Late Mrs.Theresa,
Aged about 67 years,

(2) **Mr.GNANA PRAKASH,** (PAN No.AINPP4648N)
S/o. Late Mr.D.Anthony & Late Mrs.Theresa,
Aged about 64 years,

(3) **Mr.A.SURIA PRAKASH @**
SURYA PRAKASH, (PAN No.ADUPA6460B)
S/o. Late Mr.D.Anthony & Late Mrs.Theresa,
Aged about 59 years,

(4) **Mr.A.GERARD KUMAR @ A.KUMAR,**
S/o. Late Mr.D.Anthony & Late Mrs.Theresa,
Aged about 57 years,

(5) **Mr.A.DEENA DAYALAN @**
A.DEEN DAYALAN, (PAN No.ADAPD2112M)
S/o. Late Mr.D.Anthony & Late Mrs.Theresa,
Aged about 54 years.

[Signatures of the parties]

PAGE No. - 1 -



Print Date & Time : 02-05-2016 05:11:47 PM

ದಾಖಲೆ ಸಂಖ್ಯೆ : 422

ಇದೇ ದಿನದ ಮುಖಾಂತರವಾಗಿ ಸಾರ್ವಜನಿಕ ದಾಖಲೆ ಸಂಖ್ಯೆ 02-05-2016 ರಿಂದ 04.06.2016 ರವರೆಗೆ ಈ ದಾಖಲೆಗೆ ಸಾರ್ವಜನಿಕ ದಾಖಲೆ ಸಂಖ್ಯೆ.

ಕ್ರಮ ಸಂಖ್ಯೆ	ವಿವರ	ಮೊ. 4
1	ಮೊ. 422	240000.00
2	ಮೊ. 422	1190.00
3	ಮೊ. 422	40.00
4	ಮೊ. 422	241230.00

By: Mr. S. Mohammed Khaleel ಸಹಿ ಸಂಖ್ಯೆ

ಹೆಸರು	ಚಿತ್ರ	ಸಹಿ	ಮೊ. 4
Mr. S. Mohammed Khaleel			241230.00

ಮಾನ್ಯತೆಗೆ ಪಾತ್ರ

ಮಾನ್ಯತೆಗೆ ಪಾತ್ರ

ಕ್ರಮ ಸಂಖ್ಯೆ	ಹೆಸರು	ಚಿತ್ರ	ಸಹಿ	ಮೊ. 4
1	Mr. S. Mohammed Khaleel			241230.00
2	Mr. Syed Arman			241230.00

PAGE No. - 2 -



Thank You