eSign Online Digital Signature

Mini Conference

Ensuring Legally Significant Trusted Transboundary Electronic Interaction

29 March 2017

Content

- Context & need for eSign in India
- What is eSign
- Potential use cases
- How eSign works

Information Technology Act

- The Indian IT Act, 2000 provides legal sanctity to Digital signatures and the electronic documents that have been digitally signed
- Treated at par with paper documents signed in the traditional way
- The IT Act provides the basic legal and administrative framework for e-commerce, and promotes its growth by creating trust in electronic environment

Controller of Certifying Authorities

- The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities
- Certifying Authorities (CAs) issue Digital Signature Certificates(DSC) for authentication of users in cyberspace
- The Certifying Authority (CA) is required to verify the credentials of the applicant as stated in the Application Form and supporting documents

The existing solution for issuing DSCs is expensive and non-scalable, paving way for managing DSCs through the new digital identity platform Aadhaar

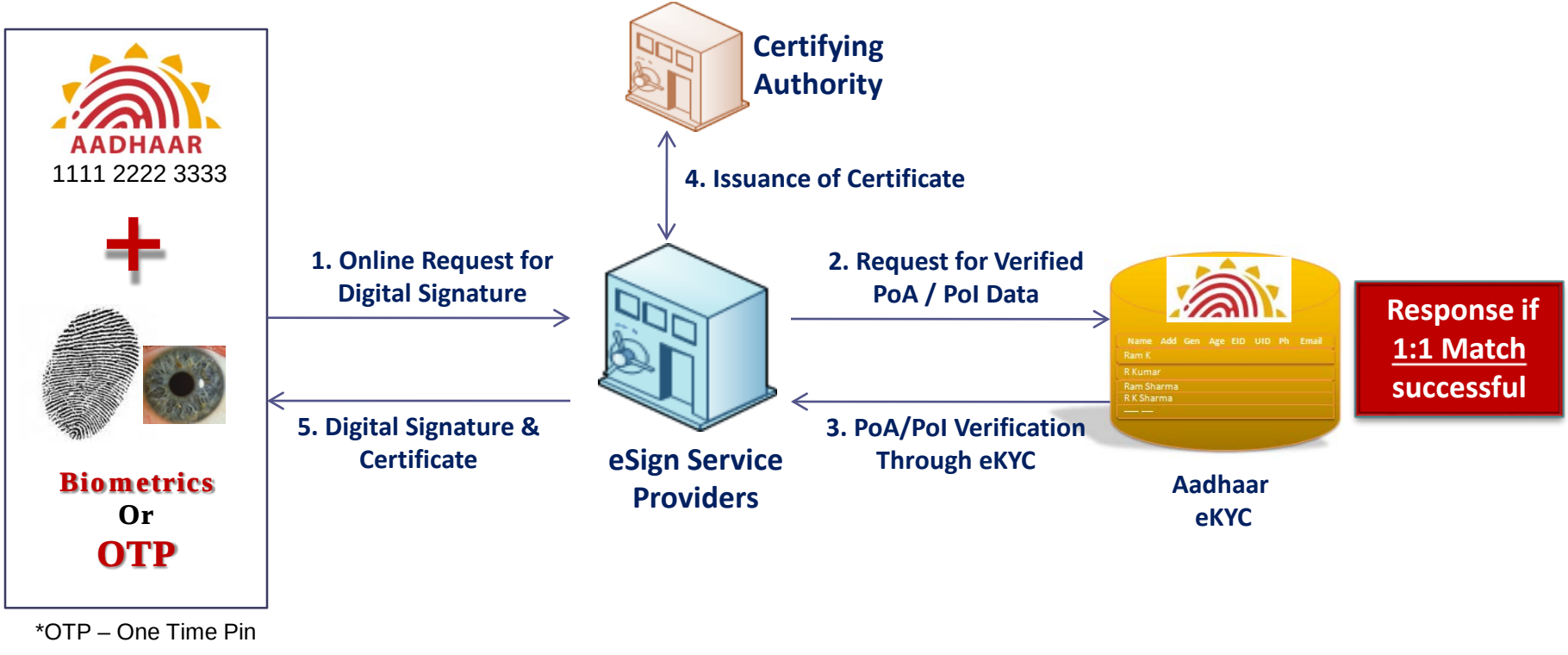
Current procedure for issuing Digital Signature Certificates (DSC) requires physical verification, document based identity validation, and issuance of physical dongles

This makes DSC expensive, time taking and non-scalable to cater to one billion people – adoption is largely limited for business usage

eSign is an online service that facilitates instant issuance of DSC through Aadhaar authentication

In eSign, instead of giving physical documents, Aadhaar holder authorizes UIDAI to provide eKYC data to Certifying Authorities – making the process instant, paperless and cost effective

eSign is envisaged to be a giant leap towards large scale adoption of digital signature and hence paperless transactions



eSign Service

eSign facilitates digitally signing a document by an Aadhaar holder using an Online Service. Aadhaar ID is mandatory for availing this service

Digital Signature is created using authentication of consumer through Aadhaar eKYC service

eSign is an integrated service that facilitates issuing a Digital Signature Certificate and performing Signing of requested data by authenticating Aadhaar holder

Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 has been notified to provide the legal framework

eSign Service – Benefits

1.	**Save cost and time**	Aadhaar e-KYC based authentication
2.	**Improve User Convenience**	Flexible and fast integration with application
3.	**Easy to apply Digital Signature**	Biometric or OTP (optionally with PIN) based authentication
4.	**Verifiable Signatures and Signatory**	Mandatory Aadhaar ID
5.	**Legally recognized**	Integrity with a complete audit trail
6.	**Managed by Licensed CAs**	API subscription Model
7.	**Privacy concerns addressed**	No key storage and key protection concerns
8.	**Simple Signature verification**	Suitable for individual, business and Government
9.	**Short validity certificates**	Immediate destruction of keys after usage

Comparison of existing solution for issuing DSCs to proposed eSign solution

As-Is DSC Process

- Stakeholders in DSC issuance:
  - Certificate Holders
  - Relying Parties
  - Certifying Authorities (for certifying public key, publishing certificates, providing DSC to subscribers)
  - Registration Authorities (for verifying documents, issuing passcodes)
- Activities:
  - One time: Physical verification (PoA, PoI), dongle issuance

To-Be eSign Process

- Stakeholders in eSign issuance:
  - Aadhaar holders (= Certificate holders)
  - Application Service Provider (= Relying Parties
  - eSign Service Provider
  - Certifying Authority (CA operates as ESP)
  - UIDAI (already has verified PoI, PoA data)
- Activities:
  - One time: None
  - For every transaction: eSign request, which invokes eKYC request to UIDAI's CIDR

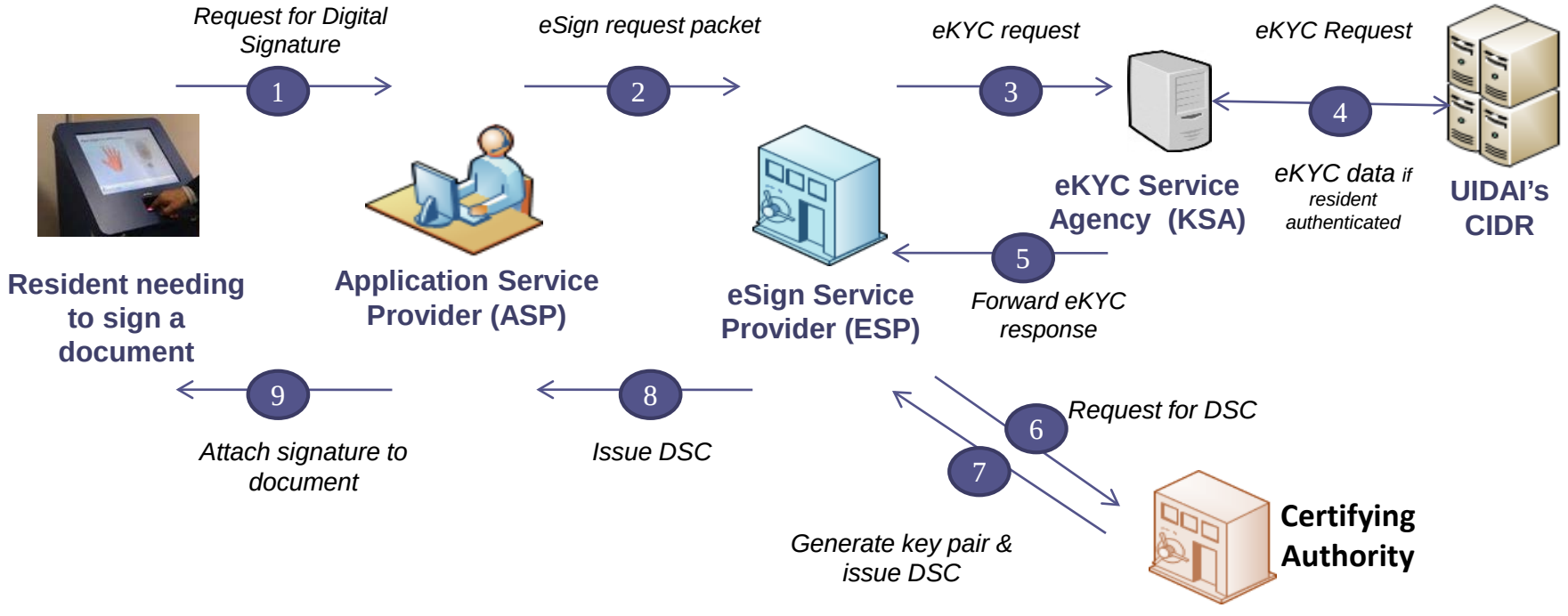
Potential Use Cases

Opening Bank Accounts / Insurance or credit products / SIM Cards	• A prospective customer can get instant bank account / insurance or credit product / SIM card through a bank ATM / telco outlet through digitally signing the request packet and obtaining data online through eKYC • If required, in parallel, bank may look up CIBIL (or equivalent) score online to validate credit standing
Filing Income Tax Returns	• Instead of current 2-step process followed by a large number of citizens (filing returns online and then printing ITR Form, signing and sending by post to CPC), the returns can be digitally signed online in one-step process
Applying for Passport / Voter Card / Ration Card	• A citizen can apply for passport or any other such card online through digitally signing the request packet • The basic demographic data available through eKYC can be used as PoA/PoI; other validation / authorization process of the department would be followed in respect of digitally signed request

Examples of some of the transactions that have the potential to migrate to online paperless transactions through eSign

S. No	Department/Sector	Service	Volume projections (per annum)
1.	Digital Locker	Self Signing	20 million
2.	Income Tax	Pan Issuance	10 million
		Return Filing	40 million
3.	Financial Sector	Account opening in Banks	100 million
		Account opening in Post Office	20 million
4.	Passport	Issuance	6 million
		Reissue	4 million
5.	Telecom	New Connection	60 million
6.	Rural Health Insurance	Application	3 million

How eSign works



Key Stakeholders and Their Engagements

Application Service Providers (ASP)	• ASPs need to engage with ESPs • ASPs have to comply to the e-authentication Guidelines laid down by CCA • Examples of ASPs include banks, insurance companies, government departments, telcos etc
eSign Service Provider (ESP)*	• Only Certifying Authorities (CAs) can become ESPs. To offer eSign services, they need to adhere to the e-authentication guidelines laid down by CCA • ESPs need to apply to UIDAI for becoming KUA and follow processes prescribed thereof • ESP needs to engage with KSA to avail UIDAI's eKYC service
Certifying Authorities(CA)	• CA issue DSC to applicant holding Aadhaar Number

* When the ecosystem scales up, there is a possibility of an ASP availing services from multiple ESPs. In that case, there would be a gateway provider (much like online payment gateways) which would allow the citizen / ASP to choose a particular ESP basis varying business needs, user preferences etc.

Key Stakeholders and Their Engagements (Contd.)

eKYC Service Agency (KSA)	• A entity desiring to become KSA needs to approach UIDAI • UIDAI's website has a list of approved KSAs
Unique Identification Authority of India (UIDAI)	• UIDAI has the mandate of providing a Unique Identification Number (Aadhaar) to all residents • Aadhaar is issued basis biometric (fingerprint & iris) de-duplication; Aadhaar database contains basis demographic data for residents – name, gender, age/DOB, address • Through eKYC service of Aadhaar, a resident (after being duly authenticated) can authorize UIDAI to share his/her demographic data & photograph with required service providers
Office of Controller of Certifying Authorities (CCA)	• CCA is appointed under IT Act to promote the use of Electronic Signature in the Country • For eSign Online Electronic Signature Service, CCA issues the e-authentication guidelines and also facilitates the eSign API.

Based on the authentication attribute used for obtaining eSign service, two eSign classes are defined*

OTP Based eSign request	• In this case, the DSC issued is based on valid OTP submitted by the applicant
Biometric Based eSign request	• In this case , the DSC issued is based on valid biometric input being provided by the applicant
Additional factor of authentication such as PIN	• ASP may choose to opt for an additional factor of authentication for issuing eSign • This would be ASP's prerogative and is to be offered by a future Gateway service provider

* Similar to the current system of DSC where the relying party chooses applicable class of DSC, choosing eSign class is also ASP's prerogative.

Further, since some of the ASPs are expected to use eKYC data for signing up their customers / beneficiaries, various use cases for eSign can be divided into two categories basis the data need of ASP

- Category 1: ASP requires only digital signature and not eKYC data
  - Example: Filing income tax returns

- Category 2: ASP requires eKYC data as well as digital signature
  - Example: Opening bank account

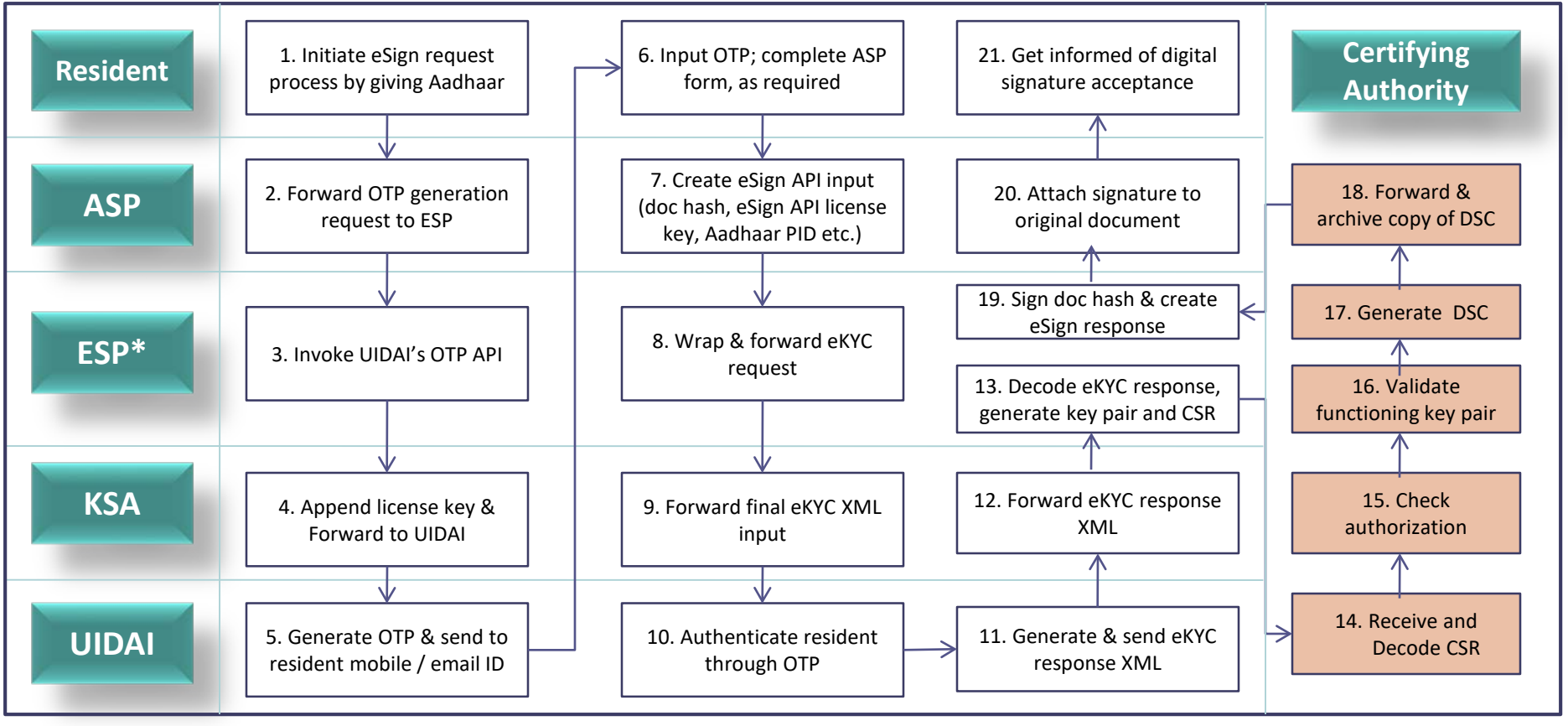
To ensure convenience to customers/beneficiaries and to reduce the overall transaction time & cost, the solution is being designed for one time eKYC for every transaction & same eKYC response data being used by both ASP & ESP.(Provided sharing of eKYC is allowed by UIDAI)

The detailed workflow for interaction between stakeholders would depend upon the authentication factor used & need for eKYC data at ASP end..

	Category 1: ASP Doesn't Need eKYC Data	Category2: ASP Needs eKYC Data#
OTP Based	**Use Case 1*** 1. Filing Income Tax returns 2. Digital locker request & access 3. Driving license renewal	**Use Case 3*** 1. Bank /insurance account opening 2. PAN issuance 3. Voter card registration
Biometric Based	**Use Case 2*** 1. Application for various certificates (marriage, caste, birth, death etc)	**Use Case 4*** 1. New telecom connection 2. Passport renewal / request

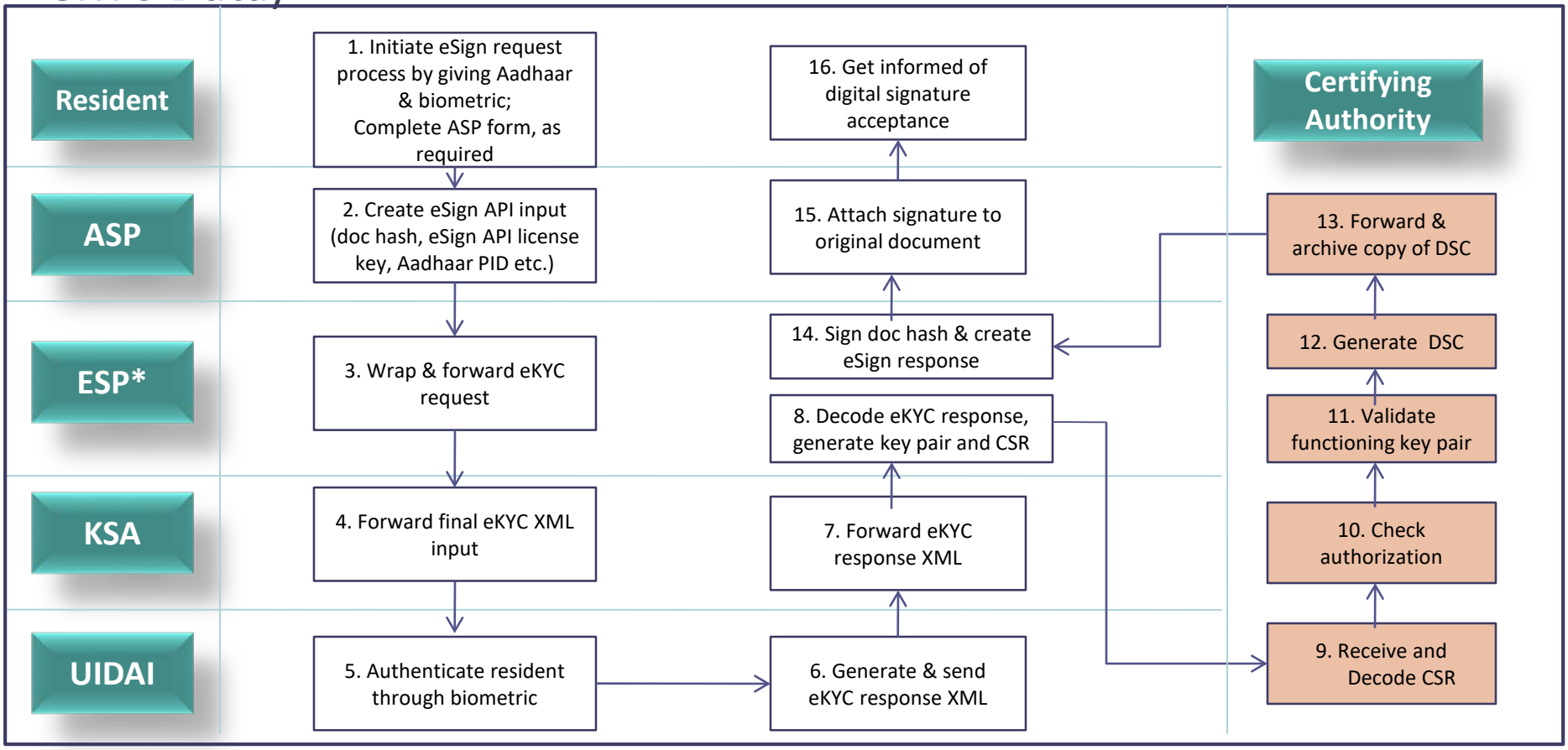
* The examples of use cases under various categories & classes are only illustrative in nature. Decision regarding required class (authentication attribute) and category (need for eKYC data) is ASP's business prerogative.
# If ASP needs eKYC data, ASP needs to sign up as KUA with UIDAI and make arrangements with a KSA.

Use Case 1: OTP Based, Category 1 eSign (ASP Doesn't need eKYC Data)



*ESP is the AUA/KUA in this scenario

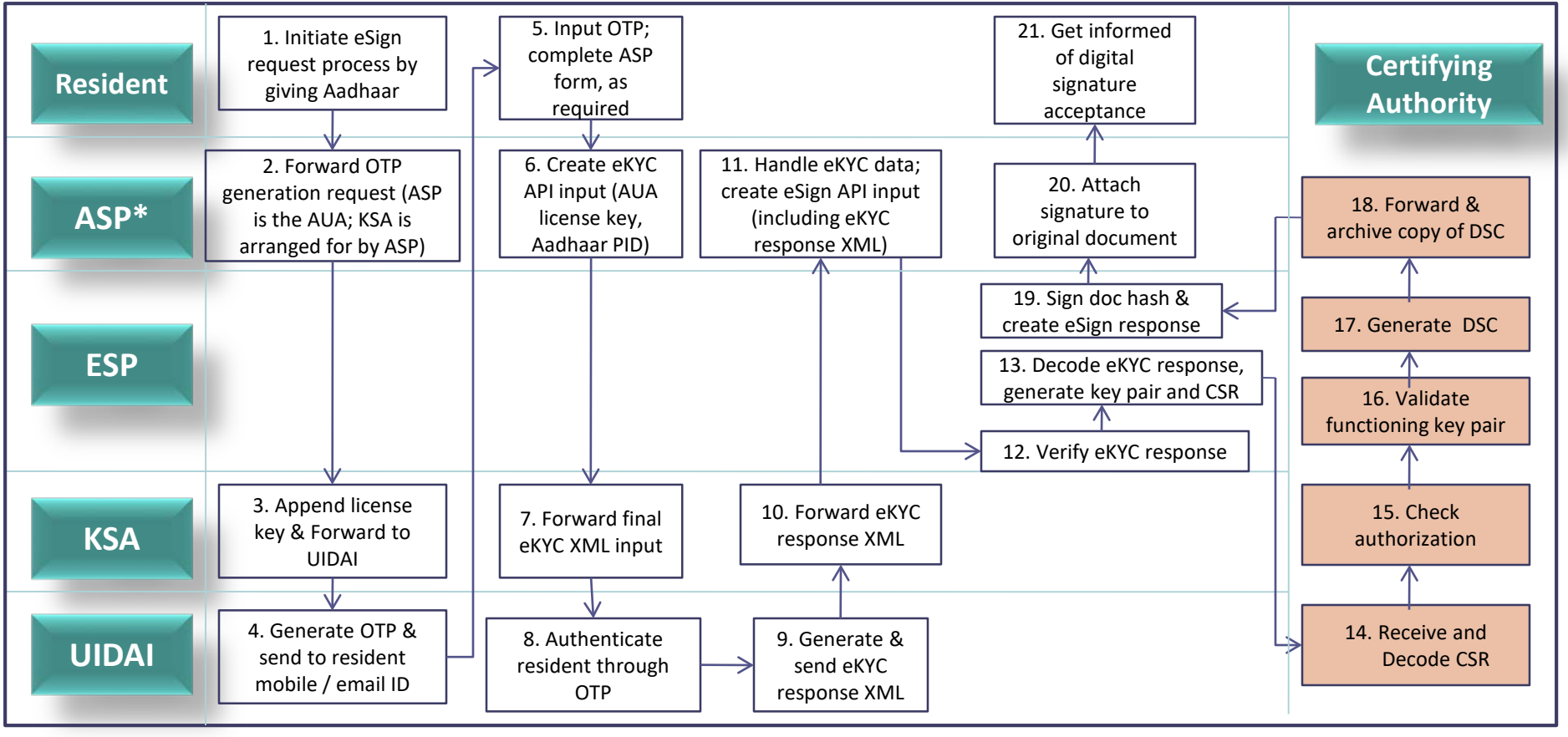
Use Case 2: Biometric Based, Category 1 eSign (ASP Doesn't need eKYC Data)



*ESP is the AUA/KUA in this scenario

Certifying Authority Functions

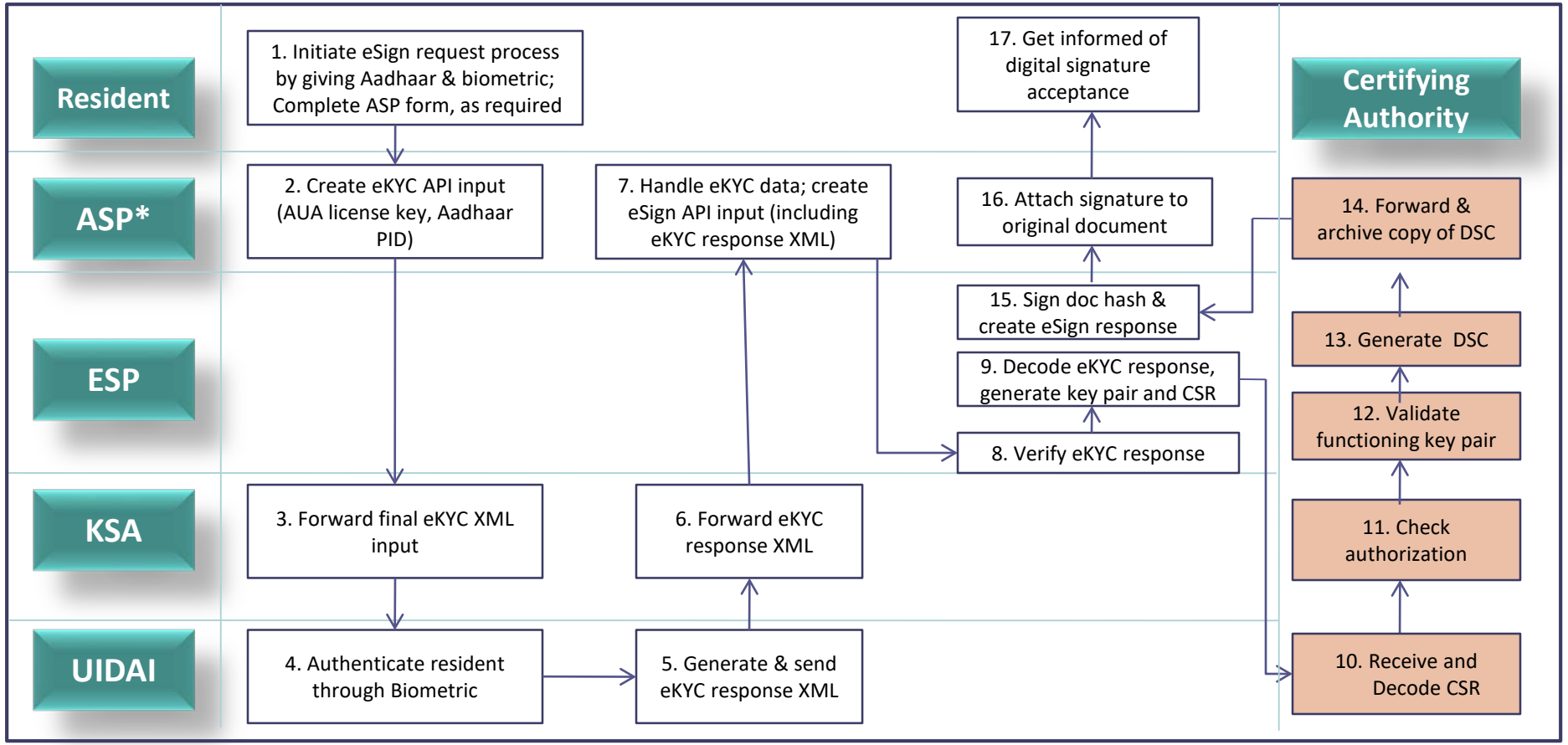
Use Case 3: OTP Based, Category 2 eSign (ASP needs eKYC Data)



*ASP is the AUA/KUA in this scenario

Certifying Authority Functions

Use Case 4: Biometric Based, Category 2 eSign (ASP needs eKYC Data)



*ASP is the AUA/KUA in this scenario

Availing eSign Service: Steps to be followed by an **ASP**

1. Apply to ESP for integrating eSign Service in their application
2. If the ASP needs eKYC data, engage with UIDAI to become an AUA
3. Update client and backend applications to provision for eSign; Perform testing in the staging environment
4. Submit audit report and checklist to ESP
5. Obtain license key and test in the production environment

Availing eSign Service: Steps to be followed by an **ESP**

1. Use the eSign API to develop technology solution
2. Engage with UIDAI to become a KUA identify a KSA
3. Perform testing in the staging environment
4. Prepare audit reports and checklists
5. Obtain license key and test in the production environment

Thank You!

Tahseen A Khan
UN/CEFACT Vice Chair
takhan@nic.in