

CCA e-Sign API Specification Part 1 : E-Signature for online e-KYC

**Version 1.0
27 March 2022**



**OFFICE OF THE CONTROLLER OF CERTIFYING AUTHORITIES
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology**


Document Control

Document Name	e-Sign API Specifications
Status	Release
Version	1.0
Release date	
Last update	
Document Owner	Controller of Certifying Authorities (CCA), Bangladesh.

Copyright © CCA-Controller of Certifying Authorities, 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of CCA-Controller of Certifying Authorities.

Trademarks and Permissions

 CCA and other CCA's trademarks are trademarks of Controller of Certifying Authorities of Bangladesh.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

CCA-Controller of Certifying Authorities

Address:	Government of the People Republic of Bangladesh Office of the Controller of Certifying Authorities(CCA) E-14/X, ICT Tower(1st floor) ICT Division, Agargaon, Dhaka, 1207
Website:	http://www.cca.gov.bd/
Email:	info@cca.gov.bd

GA

Basim

GA

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue

Version	Date	Reason for issue	Issued By	Reviewed By

CA

DL

DL

Table of Contents

Document Control.....	2
Change History	3
Changes in Issue.....	3
1.0 Summary	1
1.1 Audience	3
1.2 Objective.....	3
1.3 Definition.....	3
1.3.1 e-Sign	3
1.3.3 Business Application Owner (BAO).....	4
1.3.6 e-Sign Service Provider (ESP).....	5
1.3.7 Controller of Certifying Authorities (CCA).....	5
1.3.8 Certifying Authority (CA)	5
1.3.9 Certification Practice Statement (CPS).....	6
1.3.10 Personal Information.....	6
1.3.11 Biometric Personal Information.....	6
1.3.12 API	6
1.4 e-Sign service in detail	6
2 Understanding e-Sign Service.....	9
2.1 e-Sign Service at a glance.....	9
3 e-sign Service API.....	9
3.1 API Functionalities and features.....	10
3.2 e-Sign Usage scenarios.....	11
3.3 e-Sign using e-KYC made by ESP	11
3.4 Signing Process.....	14
3.4.1 Basic e-Sign	14
3.5 e-Sign Response	14
3.5.1 Business Application calls ESP's API (Flow-1)	14
3.6 e-Sign API: Submit Data to e-Sign Service.....	15
3.6.1 API for Submitting Signing Request	15
3.6.1.1 Request Format	15
3.6.1.4 Request Parameters	16
3.6.1.5 Sample JSON Request Data (e.g.)	18
3.6.1.6 Digital Signature of the JSON Request Data	19
3.6.1.8 Response Parameter	20
3.6.1.10 Sample Response(e.g.)	21
3.7 e-Sign: User Authentication.....	21
3.7.1 ESP User Authentication URL.....	21
3.8 e-Sign API: Check Signing Status and Fetch Result	22
3.8.1 API for Getting Signing Value (Flow-1).....	22
3.8.1.1 Description	22
3.8.1.2 Request Parameters	23
3.8.1.3 Sample Request.....	23
3.8.2 Response Parameters	23
3.8.3 Sample Response (e.g.).....	24
4 BA API Specification	24
4.1 BA Verification Response API	24
.....	25
4.1.1 Request Parameters.....	25

4.1.2 Response Parameters	25
Sample Response	26
5 Abbreviation	27

CA

WPL

CA

1.0 Summary

Controller of Certifying Authorities (CCA) is working as one of the key organizations for establishing “Digital Bangladesh” since 2011. CCA has developed necessary Rules, Guidelines for Public Key Infrastructure (PKI), established the Root CA infrastructure, and completed the license issuance process of a Certifying Authority (CA).

All 6 licensed CAs certify the authenticity of the content & identity of the signer that is legally accepted under the law of Bangladesh (ICT Act & CCA Rule & Regulations). CCA has published the recent e Sign guideline (e-Sign guideline for the Certifying Authorities (CAs) 2020, V1.01). As a licensed CA all CAs are given the opportunity to become E-Sign Service Provider (ESP). Considering the various technical interoperability, best practices of integration, CCA is willing to publish a specification standard for e-Sign API.

Developers can build a variety of different integrations with e-Sign using a web services API for communications. A web service is a standards-based, secure and scalable method of establishing communications between systems over the Web. Once built, integrations allow users to initiate the e-signing experience entirely from within the external application. Developers can also incorporate the functionality of e-Sign into their business applications by embedding the e-Sign plug-in or module within those applications. Business application can also receive status updates in real-time for transactions initiated using e-Sign. These business applications can also retrieve and store copies of the signed agreements.

This document is issued under sections 19 (b) and 19 (d) of the Information and Communication Technology Act 2006 & Rule 7 of IT (CA) Rules 2010. It lays down the standards to be adhered to by all the licensed CAs in providing e-Sign service to the subscribers.

This document covers the following areas:

- How to use the e-Sign interface to establish integration with an external application.
- Information on document keys and the configuration of OAuth or SSO.
- Various scenarios for using the e-Sign APIs to integrate with an application.

- Information on integrating e-Sign and external applications by embedding the e-Sign API, Plugin, or module into that business application.
- How to send information about events or actions in e-Sign to business application.

The real-time e-KYC service makes it possible for service providers to provide instant service delivery to eSign Users which otherwise would have taken a few days for activation based on the verification of KYC documents, digitization, etc.

e-Sign facilitates digitally signing a document by an e-Sign user through a **business application**. While authentication of the signer is carried out using e-KYC, the

signature on the document is carried out on an ESP server. The service shall be offered only by Certifying Authorities. The e-Sign is an integrated service that facilitates issuing a Signature Certificate and performing Signing of requested data on basis of the authenticated e-KYC response. The certificate issued through the e-Sign service will have either basic as one time or advanced as multiple usages but time-bound.

e-Sign facilitates digitally signing a document by an eSign user using an Online Service. While authentication of the signer is based on e-KYC response and confirmation by CA, the signature on the document is carried out on an **ESP server**, which is the e-Sign provider. The 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 on basis of the authenticated e-KYC response. The eSign Service shall be implemented in line with e-KYC Guideline for CA Operators 2021 issued by Controller. The certificate issued through the eSign service will have a **limited validity period** and is only for **the one-time signing** of requested data.

1.1 Audience

This is a technical document and is targeted at Application Service Owner who require signing of digital document(s) in their application as per instruction of the e-Sign User.

This document is intended for:

- ★ All the CA & Sub CA

- * Installation and commissioning engineers of CA & Sub CA
- * Technical support engineers of CA & Sub CA
- * All Business Application Owner for their Business Applications

1.2 Objective

The objective of the document is to introduce e-Sign service in Bangladesh under the applicable laws and regulations to accommodate e-KYC for immediate document signing service. In Part-1 Basic eSign which need to communicate with ESP is stated.

1.3 Definition

1.3.1 e-Sign

A form of electronic signature or digital signature provided and certified by CAs as per ICT Act 2006 clause 2(1) and IT (CA) Rules 2010 where the user's private key is kept on e-Sign Service Provider CA's end, where the user has sole control of it through appropriate ecosystem.

"eSign" or "eSign Service" is an online Electronic Signature Service in which the key pair generation, certification of the public key by the CA and digital signature creation for electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service based on successful authentication of individual using e-KYC services.

1.3.2 e-Sign Subscriber

"eSign User or eKYC user or subscriber" is an individual requesting for eSign online Electronic Signature Service of eSign Service provider. This individual shall be using the application of Business Application Owner and represents himself/herself for signing the document under the legal framework. For the purposes of Electronic Signature Certificate by the CA, the eSign user shall also be the 'applicant/subscriber for digital certificate', under the scope of ICT Act.

1.3.3 Business Application Owner (BAO)

The owner of the business application owner software or application where e-sign will be integrated into the workflow. An organization or an entity using eSign service as part of their application to digitally sign the content.. Examples include Government Departments, Banks and other public or private organizations.

Business application (BA)

The business application software or application where e-Sign will be integrated into the workflow.

The example Business Applications might be a Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Document Management System (DMS), any workflow management software etc. Business applications may have office document (doc, excel, power point etc), PDF, web forms etc. where e-Sign will be applied. These business applications can have intra and inter-company usage or any public use. End users may register to the e-Sign platform directly or through any such business application. BA would be connected to the e-Sign platform through API in the background by secured & encrypted means.

1.3.4 e-KYC

Electronic Know Your Customer (e-KYC) is an electronic automated method used to verify and authenticate the identity of a e-Sign Subscriber as defined in Rule 2j) of IT (CA) Rules 2010.

Electronic Know Your Customer or "e-KYC" means the transfer of digitally signed demographic data such as Name, Address, photograph etc of an individual collected and verified by e-KYC provider on successful authentication of same individual

1.3.5 e-KYC Service

Identity Verification service provided by CAs as per Rule 24 (e) of IT (CA) Rules 2010.

e-KYC provider shall mean any e-KYC provider listed in e-KYC Guideline for CA Operators, 2021. eKYC provider is responsible for eKYC user

management and authentication eSign user. In case CA maintains eSign User Accounts of subscribers/eSign user, the security and privacy will be applicable as per the provisions specified under IT Act.

1.3.6 e-Sign Service Provider (ESP)

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 will facilitate subscriber’s key pair-generation, storing of key pairs on hardware security module and creation of digital signature. ESP must be integrated with a CA for the purpose of obtaining Signature Certificate for the generated Key-pair.

The CAs and their Sub-CAs Licensed by CCA can provide e-Sign Service under section 2 (32) and 2(34) of ICT Act 2006 and as per the Rule 21 of IT (CA) Rules 2010.

1.3.7 Controller of Certifying Authorities (CCA)

Organization established under ICT Act 2006 to govern the certificate authorities and regulate and electronic signature landscape of Bangladesh

1.3.8 Certifying Authority (CA)

An organization or an entity licensed under CCA for issuance of Digital Certificate and carrying out allied CA operations.

CCA Licensed Body/Bodies working under section 2(32) of ICT Act 2006 and providing electronic signature, digital signature, e- Sign Certificate & related services under section 36 of ICT Act 2006.

1.3.9 Certification Practice Statement (CPS)

Certification Practice Statement submitted by the Licensed CAS under Rule 21(a) of IT (CA) Rules 2010 and approved by CCA.

1.3.10 Personal Information

Information relating to any person, with which he or she may be directly or indirectly identified (e.g. biometric information)

1.3.11 Biometric Personal Information

Physical & biological Information of any person such as fingerprints, retina, and particle of the eye, voice pattern, etc.

1.3.12 API

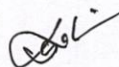
An application programming interface (API) is a computing interface that defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc.

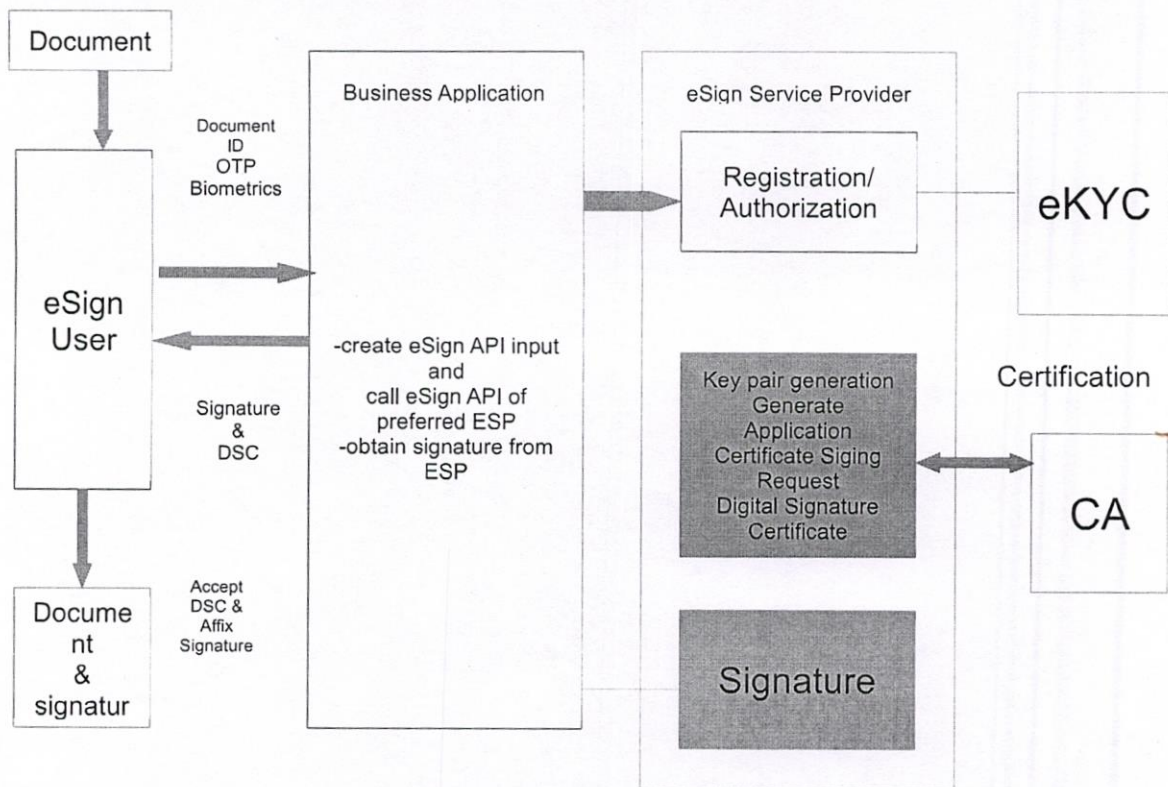
1.4 e-Sign service in detail

e-Sign will be applied by using a mobile phone or email. For that purpose, the user's mobile number or email has to be registered with the CA after e-KYC verification with the **national ID system of Bangladesh**. The registration process will be automated & instant.

The user will apply e-Sign on electronic content through a 3rd party **Business Application, which** refers to the business application software or application where e-Sign will be integrated into the workflow.

In this category of eSign eSign user initiate eSign process by placing In this category of eSign eSign users initiate the eSign process by placing Document ID (hash of the document) with OTP and his/her biometrics to **Business Application (BA)**. BA hands over to ESP to authenticate the user. After getting an e-KYC positive response, then only prepare the signing process by creating key-pair, collect DSC from CA. ESP then signs the hash and pass to BA and then to the user.





ESP returns signature to BA and BA pass to eSign user for final affixing of signature with a document. Private key is destroyed just after the signing of the document. Public key is available with DSC.

In this format, eSign users can sign infrequent on their documents when they feel necessary. In an online format, users can sign whenever he/she wants to sign as it may need a long process of verification.

In this case, the private keys are destroyed just after the sign of the document. Only one document should be signed by these processes to reduce the vulnerability of ESP.

BA will send the content to the ESP of the CA e-Sign platform along with the user credential for signing. The ESP platform will receive that and send an OTP to the end-user through SMS or email directly to the user to their registered mobile number or email. End-user will have to enter that OTP to BA portal interface, upon receiving ESP will verify the OTP and apply the electronic signature to the electronic record and publish the Certificate.

[Handwritten signature]

[Handwritten signature]

[Handwritten mark]

This will certify the Authenticity of the record and the identity of the end user. All electronically signed content or records are accepted by law in Bangladesh and can be used in place of Ink signature.

End User Registration	End User Verification through NID Integration	e-Sign Type Selection
Business Application Connectivity & Integration through API	e-Sign Issue, Apply, (Invoke), Certificate Generation	Business Application Operation & Life Cycle Management
e-Sign Life Cycle Management	Customer Support (User & BA)	Internal Admin, Accounting, Management & Reporting

The overview of e-Sign Service is shown in the table.

2 Understanding e-Sign Service

This section describes e-Sign Service, some of the envisioned usage scenarios, and working details. Technical details follow in subsequent sections.

2.1 e-Sign Service at a glance

A simple data flow diagram shows the e-Sign service in Following Figure.

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

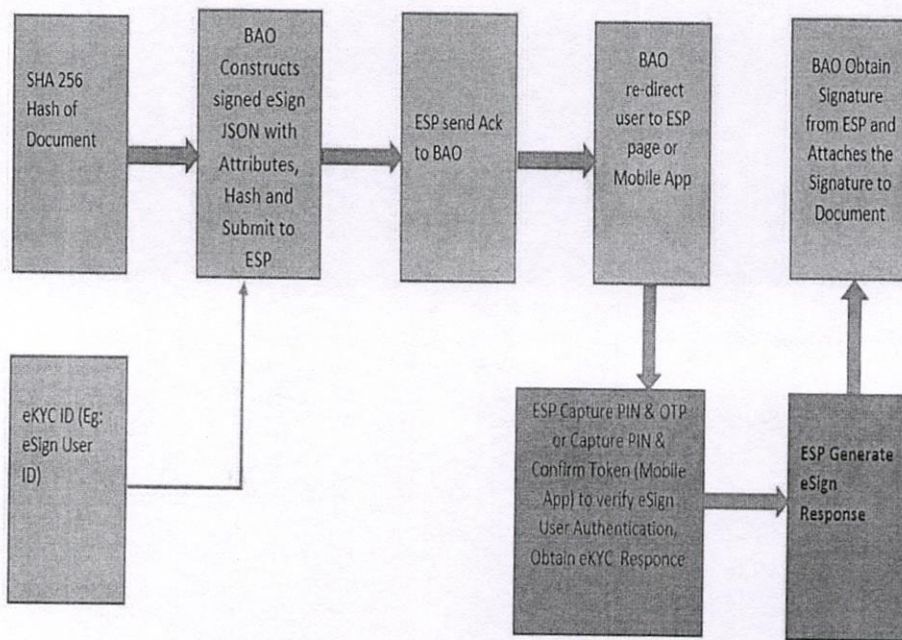


Figure 1: Data flow diagram

3 e-sign Service API

e-Sign service is exposed as stateless service over HTTPS. Usage of open data format in JSON and widely used protocol such as HTTPS allows easy adoption and deployment of this service. To support strong end to end security and avoid request tampering and man-in-the middle attacks, it is essential that the requests and responses are digitally signed.

The usage of HTTPS shall ensure transport layer encryption, while digital signing of JSON shall ensure integrity & authenticity of data.

The suggested method for obtaining authenticated e-KYC response is ESP facilitates authentication of the e-Sign user by calling the authentication URL of the e-KYC provider. The e-KYC response will be received by ESP and ESP performs e-Sign on the e-Sign request received from BAO within permissible time limit.

3.1 API Functionalities and features

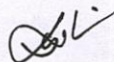
- 1 API request and response should be asynchronous;

[Handwritten signature]

[Handwritten signature]

[Handwritten mark]

- 2 Request and Response parameters should allow JSON data format;
- 3 Any authentication required by the user can be done by using Web Authentication Page or by using mobile app;
- 4 Multi-Page document signing should be available;
- 5 All API communication / request-response should be done over HTTPS;
- 6 All API should follow POST method;
- 7 Each API should have versioning, transaction id, waiting period, redirect URL, signing algorithm, response URL;
- 8 Large document should be accessible using HTTPS URL and accessible by using authentication;
- 9 In the e-Sign User account for Government Officials, along with other data, it should use/allow Nothi ID during account creation;
- 10 Each API should have pre-defined error code;
- 11 Each API should have pre-defined status code;
- 12 There should be status checking API;
- 13 Each timestamp should be GMT+6 also time stamp should follow unified format like as per ISO standard;
- 14 Signer ID for Government officials should allow E-Nothi/D-Nothi ID;
- 15 All URL should follow HTTPS;
- 16 Hashing algorithm should be SHA256;
- 17 All GEO code in communication should follow BBS standard;
- 18 All Personal data like gender, DOB, should follow CCDS standard;
- 19 charset should follow Unicode UTF-8.



3.2 e-Sign Usage scenarios

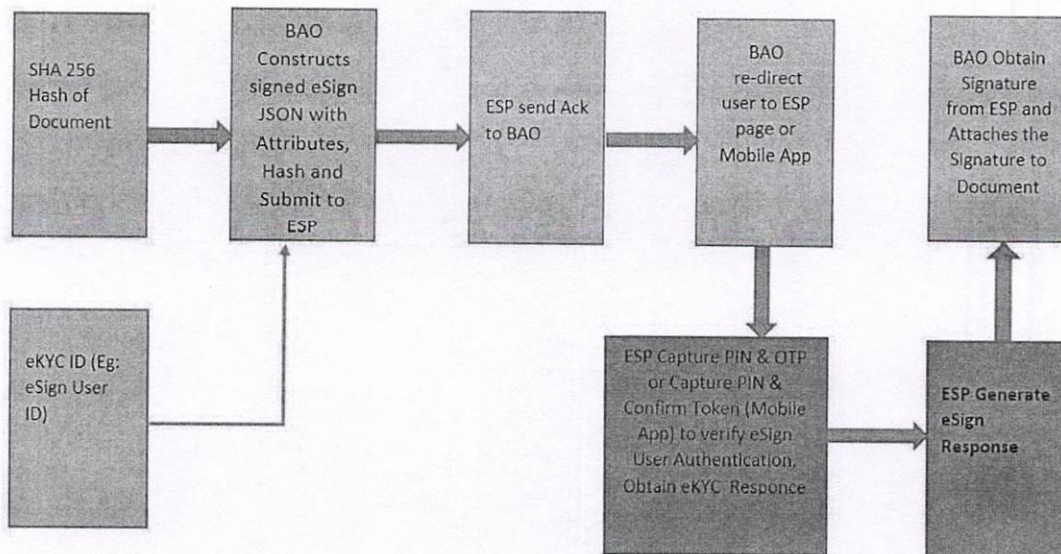
The API specifications remain common for all e-Sign Service providers. However, the parameter values that will vary for each ESP are 'e-Sign Service URL' and 'BA ID' (Unique BA ID provided by the ESP).

The e-Sign service API can be used in the scenario where BA initiates e-Sign requests and ESP authenticates users for e-KYC before e-Sign through the CA provider.

3.3 e-Sign using e-KYC made by ESP

BA calls the ESP signing request API, later (post signature authorization by subscriber) ESP will call back BA and provide the signature status and data. As ESP is part of CA, for this reason, the Private Key generated in the premise of ESP is the same as CA. Key does not leave the secure premise of the CA. As CA is specialized for passing Certificate of Public Key, ESP is responsible for **Key-pair generation**, signing the **document hash**, and collection of **certificate of the public key**. ESP will generate a signature within the **life of the Private key** as stated in a certificate by the CA.

Flow of e-Sign process using this option is shown as following.



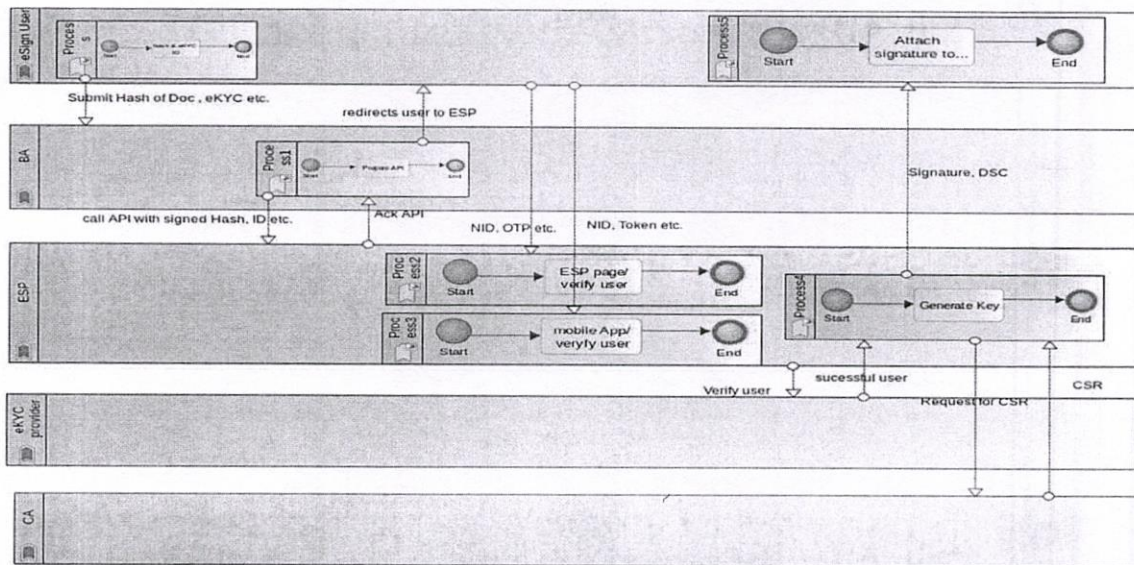


Figure 2: BPMN Diagram of e-Sign service

In this scenario:

1. **Business Application** creates the document hash (to be signed)
2. **Business Application** calls e-Sign Request API to submit signing request
3. ESP verifies the **Digital signature of the Business Application** and the validity of the input data
4. ESP acknowledges the request back to **the Business Application** by providing a Transaction ID of the request
5. Business Application redirects the user to ESP's authentication page. Alternatively, users can use ESP's mobile app to authenticate. Business Application shall suitably display necessary information.
6. ESP displays authentication page (if web flow) or notifies the ESP mobile app for device authorization

[Handwritten signature]

[Handwritten signature]

[Handwritten mark]

7. ESP performs authentication using OTP and PIN and gets e-KYC information from its e-KYC service
8. ESP calls Business Application's 'BA Verification Response URL' with the e-KYC verification status
9. If Business Application has provided 'BA Callback URL', ESP redirects the user back to Business Application's web page (web flow)
10. Now the signing process will be done at ESP. The private key used for creating the electronic signature is stored in hardware cryptographic token which is of one time use.
11. ESP asks CA for the certificate of the public key using Certificate Signing Request (CSR).
12. ESP verifies the Digital signature and validity of the input data

The BPMN diagram for e-Sign using e-KYC made by ESP is shown in the given Figure 3.

3.4 Signing Process

3.4.1 Basic e-Sign

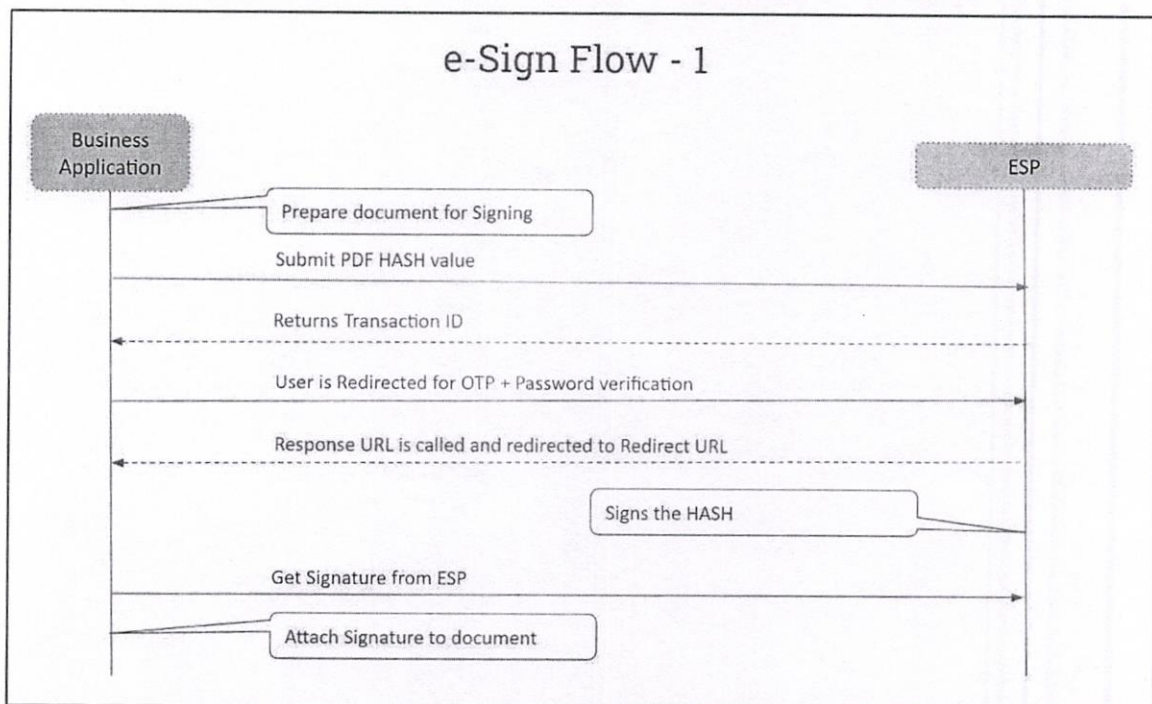
- 1 After getting positive response from e-KYC server on the ESP's requests to e-KYC with credentials to verify the e-Sign user as supplied by BA, ESP will start eSign service.
- 2 ESP creates a new key pair and CSR for the e-Sign user. The private key used for creating the electronic signature is stored in hardware cryptographic token which is of one time use.
- 3 ESP calls the CA service with CSR and gets a Digital Signature Certificate for the e-Sign user with a short time to live.
- 4 ESP signs the HASH value as supplied by BA with in this time frame as per.
- 5 ESP will destroy the private key after the signing.

3.5 e-Sign Response

Business Application Owner can get e-Sign response from ESP in two ways:

3.5.1 Business Application calls ESP's API (Flow-1)

- 1 Business Application calls e-Sign Response API to get e-Sign response data
- 2 Business Application receives the document signature and the e-Sign user's Digital Signature Certificate
- 3 Business Application attaches the signature to the document



3.6 e-Sign API: Submit Data to e-Sign Service

3.6.1 API for Submitting Signing Request

3.6.1.1 Request Format

URL: IP or URL shared by ESP to BAO

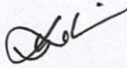
Request Data: JSON formatted data signed using JSON Web Signature (JWS)

3.6.1.2 Request **method**

The request can only be submitted by using the HTTPS method POST at present.

3.6.1.3 Encoding

HTTPS request and response are UTF-8/base64 encoded.



3.6.1.4 Request Parameters

Parameter	Type	Size	Optional	Description
Version	String	1	Mandatory	API Version Number
BA Id	String	17	Mandatory	BA ID provided by ESP for organization identity
SignerId	String	17	Mandatory	NID/Passport/Driving License number as verified in ESP's e-KYC
SignatoryConcern or sc	String	1	Mandatory	ASP should have taken a clear consent from 'eSign user' to carry on eSign from their front ending application. This attribute represents signatory's explicit consent is obtained by ASP for using the signatory's identity and address data received from e-KYC provider to, generate and submit the electronic DSC application form to CA, creation of key pairs by ESP for signatory, submission of certificate to CA for certification, one time creation of signature on the hash along with this request, deletion of key pairs from the after applying signature. Only valid value is "Y". Check box[Y/N*] *No by default
TimeStamp	Int		Mandatory	Request timestamp in ISO format. The value should be in Bangladesh Standard Time (BST), and should be within the range of maximum 30 minutes deviation to support out of sync server clocks.
eKYCIDType	Int		Mandatory	This represents the type of e-KYC ID being used. The value can be any one out of below: 1. Porichoy = A*** https://porichoy.gov.bd/
RequestUniqueId	UID	17	Mandatory	This ID of the BA calling the API, this is logged and returned in the output for

GA

SLI

BR

			correlation. Unique id of BA's sign request for future reference i.e. unique id of document etc.
AuthMode	String 1	Mandatory	<p>Authentication Mode being used for e-KYC Authentication, either to be performed by ESP, or as already made by the BA.</p> <p>Allowed values are:</p> <ul style="list-style-type: none"> <input type="checkbox"/> OTP = 1 <input type="checkbox"/> Fingerprint = 2 <input type="checkbox"/> IRIS = 3 <p>Class of eSign Certificate will be "OTP Class" for OTP based authentication. For Fingerprint and IRIS, the class will be "Biometric Class".</p>
SignatureType	String 1	Mandatory	<p>This value represents the response signature type, where ASP can request for a specific type of signature from one of the following</p> <ol style="list-style-type: none"> 1. rawrsa 2. PKCS7(with only the signer certificate in the certificate section and no revocation information) 3. PKCS7pdf (all issuer certificates up to and including root CA certificate and CRLs/OCSP responses of each issuer certificates should be included in the response. In case, the number CRL entries are more than 5, only OCSP responses are allowed. The signature should also be time stamped using the time stamping services of CA. The revocation information should be included as a signed attribute under revocation list. 4. PKCS7complete (All issuer certificates & its revocation information in unsigned info) 5. Rawecdsa [Elliptic Curve Digital Signature

				Algorithm]
HashAlgorithm	String	6	Mandatory	"SHA256" = current fixed value
HashToSign	String	1	Mandatory	"1"=SHA256 HASH Value in base64 format
Description	String	100	OPTIONAL Mandatory	Mandatory for SignatureType="1" Description of the document to be signed
DocumentLink	String	512	OPTIONAL Mandatory	Mandatory for SignatureType="1" URL Encoded Web link of the document. This link and the description will be visible during the ESP User Authentication process
BACallbackURL	String	512	Mandatory	For mobile, it would be Blank or NULL. for web flow , URL Encoded BAO callback URL i.e. https://www.bao.com/e-Signstatus
BAVerification ResponseURL	String	512	Mandatory	ESP will send e-KYC Verification Response to BAO through this URL Format: URL Encoded i.e. https://www.bao.com/verificationstatus
BAE- SignResponseUR L	String	512	Mandatory if ESP calls BAO's API (Flow-2) to send e-Sign response	ESP will send e-Sign Response to BAO through this URL Format: URL Encoded i.e. https://www. bao.com/e-Signresponse
Language	String	2	Optional	en or bn If language is null, then use the default language.

3.6.1.5 Sample JSON Request Data (e.g.)

```
{
  "Version":"1.0",
```



```

"BAId": "BA-name",
"SignerId": "1234567890",
"sc": "Y",
"TimeStamp": "2022-03-25T04:15:27+00:00",
"eKYCIdType": "1",
"AuthMode": "13",
"HashToSign": "VGhIIHF1aWNrIGJyb3duIGZveCBqdW1wcyBvdmVyIDE=",
"HashAlgorithm": "SHA256",
"RequestUniqueId": "UNI9876543",
"SignatureType": "1",
"Description": "NDA between company A and B",
"DocumentLink": "https%3A%2F%2Fwww.BAO.com%2Fdoc%2FUNI9876543",
"BACallbackURL": "https%3A%2F%2Fwww.BAO.com%2Fe-Signstatus",

"BAVerificationResponseURL": "https%3A%2F%2Fwww.BAO.com%2Fverifica
tionstatus",
"BAE-SignResponseURL": "https%3A%2F%2Fwww.BAO.com%2Fe-
Signresponse "
}

```

3.6.1.6 Digital Signature of the JSON Request Data

Signature Format	JSON Web Signature (JWS)
Standard	RFC 7515
Algorithm	RSA SHA-256
JWS Header	{"alg": "RS256"}

3.6.1.7 Sample JWS Request Data (e.g.)

JWS of the request data would be created by the BA by the Private key of the BA.

Each BA should possess a valid key for the signing of the data.

WEcVTpdkJPEQfzxXUQPigo5UjUB1PxH5fQxIxCfr9NCb9NvS1B72Xo_
 OQwouo3OID1NRStk4_kcMPpjD4v8nAC3ADr24zIgjwLra_B5S5U2CsT
 6tSgu1VmPo_mKxUU2ykpL
 s2N7LgPXbKy-
 oPPJjqo6Q0JuwLMgOnUbrx0nuAFNNeuBk1wIffZStkFJS1VPF9u3_aIA
 g_WoRXBYd-yitGifXTS0cTDqy4twK0Id3M0IENI4t-d1oAJZSX04y-
 i3DSx5Y00
 gRYDUFajkOIgrMRiQbBjETs5rCehcUzvrxqiqV79sN1QfclQi5TuFVdFn
 3odKNGwEamg5GdbyLP_TJw

3.6.1.8 Response Parameter

BA shall get response in JSON format after calling the API for Submitting Signing Request.

3.6.1.9 Parameters in Response message body

Parameter	Type	Length	Optional	Description
Status	Int	1	Conditional	0 Success 1 refuse 2 time out Only valid when Status=0
ResultCode	Int	2	Conditional	0: successes. 1: parameter is invalid. 2: authentication error. 3 User is invalid. 4 The File does not exist. 99: other error. -1:NA. For example when user cancels or request timeout occurs

ErrorMessage	string	100	Mandatory	Error Message
TransactionId	Octat string	16	Mandatory	The new Transaction ID. BA will store it against the sign request. It will be needed while fetching the signature value.
TimeStamp	octat	8	Mandatory	TimeStamp in GMT +6.00

The TimeStamp should contain both date and time, with time zone in the form ISO standard.

3.6.1.10 Sample Response(e.g.)

```
{
  "TransactionId": "2020092212345619000023",
  "Message": "Successful",
  "Status": 0,
  "TimeStamp": "2012:04:23T18:25:43.511Z"
}
```


3.7 e-Sign: User Authentication

3.7.1 ESP User Authentication URL

URL	Shared by ESP to BA
Method	GET
Parameter	txid = Transaction ID that was returned in the response of the signing request
Sample URL	https://www.sample_esp.com.bd/auth?txid=2020092212345619000023

Once the subscriber authorizes (or cancels) the request, ESP shall

- 1 Call "BAVerificationResponseURL" to with e-KYC verification status
- 2 Redirect the user to the "BACallbackURL" with status and uniqueId parameters (web flow)

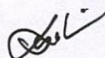
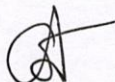
3.7.1.1 Redirection after Successful Authentication (web flow):

e.g. <https://www.BAO.com/e-Signstatus?uniqueid=UNI9876543&status=0>

3.7.1.2 Redirection after Verification Cancelled by User (web flow):

e.g. <https://www.BAO.com/e-Signstatus?uniqueid=UNI9876543&status=2>

After successful e-KYC authentication of the Signer, the Business Application Owner may use Flow-1 or Flow-2 to get Signature Value and User's Certificate from ESP.



3.8 e-Sign API: Check Signing Status and Fetch Result

3.8.1 API for Getting Signing Value (Flow-1)

3.8.1.1 Description

URL	Shared by ESP to BA
Method	POST
Content-Type	application/JSON JSON formatted data signed using JSON Web Signature (JWS)

3.8.1.2 Request Parameters

Parameter	Type	Mandatory	Description
BAId	string	y	
TransactionId	string	y	Transaction ID that was returned in the response of the signing request

3.8.1.3 Sample Request

```
{  
  "BAId": "BA-name",  
  "TransactionId": "2020092212345619000023"  
}
```


3.8.2 Response Parameters

Parameter	Type	Mandatory	Description
Status	int	Mandatory	0=success, sign done 21=SigningTaskPending 22=SigningTaskError 23=VerificationPending 996=NoSuchTask 999=System error
Message		Mandatory	Error Message
SignOutput	Base64 string	Mandatory	Base-64 Signature data <ul style="list-style-type: none">• raw or• PKCS7 (CMS) Null if Status != 0
UserX509Certificate		Mandatory	Base64 value of e-Sign user certificate (.cer)
TimeStamp	string	Mandatory	TimeStamp in GMT +6

3.8.3 Sample Response (e.g.)

```
{  
  "SignOutput": "base 64 string",  
  "UserX509Certificate": "base 64 value of user certificate",  
  "Message": "Successful",  
  "Status": 0,  
  "TimeStamp": "2012-04-23T18:25:43.511Z"
```


}

4 BA API Specification

4.1 BA Verification Response API

URL	Submitted as parameter named "BAVerificationResponseURL"
Method	POST
Content-Type	application/JSON

4.1.1 Request Parameters

Parameter	Type	Description
TransactionId	string	Transaction ID that was returned during signing request
UniqueId	string	Unique ID that was submitted during signing request
Status	int	0 = user verification successful 2 = user canceled verification
Message	string	Response related message

Sample Request

```
{  
  "TransactionId": "2020092212345619000023",  
  "UniqueId": "UNI9876543",  
  "Status": "0",  
  "Message": ""  
}
```


4.1.2 Response Parameters

Parameter	Type	Mandatory	Description
IsError	boolean	y	true false
ErrorMsg	string	y	Error Message
StatusCode	int	y	Error code if IsError = true
TimeStamp	string	y	TimeStamp in GMT +6

Sample Response

```
{  
  "IsError":false,  
  "ErrorMsg":",  
  "StatusCode":0,  
  "TimeStamp": "2012-04-23T18:25:43.511Z"  
}
```

GA

DL

GA

5 Abbreviation

API	Application Programming Interface
CA	Certifying Authority
CCA	Controller of Certifying Authorities
CSR	Certificate Signing Request
E-KYC	Electronic Know Your Customer
ESP	e-Sign Service Provider
BA	Business Application
OTP	One Time Password
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List

২৭.৩.২০২২
আব্দুল সাদিক চৌধুরী
নিয়ন্ত্রক (স্বাক্ষর-সচিব)
ইলেকট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী
কর্তৃপক্ষের নিয়ন্ত্রক-এর কার্যালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ।