**NLMC KYC Services Implementation**

NLMC will be providing bidder registration functionality in the auction portal. As part of bidder registration, NLMC requested SBI INB to provide below functionality

* Aadhar Validation (only UIDAI OTP Validation)
* PAN Validation
* GSTN Validation

INB will get the details from NLMC and will return response with sufficient fields for NLMC to do further checks (legal name check etc.) before allowing user to proceed with bidder registration. All the required INB web services will be internally implemented using EIS Services.

NLMC will decide which API to call based on the options selected by the bidder in their User Interface

INB will be implementing following services to support above requirement.

1. Aadhar Validation Request
2. Aadhar OTP Validation Request (only one attempt\*)
3. Aadhar OTP resend Request (only one resend\*)
4. PAN Validation Request
5. GSTIN Validation Request

\* UIDAI will be having flooding limits for OTP validation / Generation. Need confirmation from EIS on number of attempts allowed.

**Encryption Requirements (to be confirmed with ISD)**

All the Web services hosted by INB will be dynamic encryption with digital signature.

* Merchant and INB will share their respective public keys
* Dynamic AES key to be generated for every request or response
* Plain payload will be used for generating digital signature (SHA256withRSA) with merchant’s private key
* AES 256 Algorithm (AES/GCM/NoPadding) will be used to encrypt the payload with the AES key generated above
* Merchant will do RSA encryption (RSA/None/OAEPWithSHA1AndMGF1Padding) with SBI INB public key for the “Dynamic AES “ used for encrypting the payload

**Sample Request / Response format for all Services**

Payload will be encrypted with AES 256 dynamic key. Key will be RSA encrypted and shared in JSON Request.

**REQUEST (Payload contents will change for each service)**

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| key | RSA encrypted AES key | y |
| apirequestrefnbr | String/25 digits(recommended-DDMMYYYY+9-digit sequence number) | Y |
| payload | JSON – will be encrypted | Y |
| digitalsignature | Signature generated using NLMC private key | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr ":"recommended-DDMMYYYY+9-digit sequence number”,

"payload":

{

"apirequestrefnbr ":"Same as above”,

\*\*\*

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**RESPONSE (Payload contents will change for each service)**

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| key | RSA encrypted AES key | y |
| apirequestrefnbr | String/25 digits(ref number shared in request to INB) | Y |
| apistatus | String/25 digit(success or failure) | Y |
| apierrrocode | String /25 digit | N |
| payload | JSON – will be encrypted | Y |
| digitalsignature | Signature generated using NLMC private key | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr":"shared in request”,

"apistatus ":"success”,

"apierrrocode":"success”,

"payload":

{

"apirequestrefnbr ":"shared in request”,

"inbrequestrefnbr ":"sharedbyINB”,

\*\*\*

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**In case of encryption/decryption or signature validation errors, response will be in plain string like below.**

{

"apirequestrefnbr ":"shared in request”,

"apistatus ":"failure”,

"apierrrocode":"NLMCERR0001”

}

**Error codes (common for all services)**

|  |  |
| --- | --- |
| **Error Code** | **Description** |
| NLMCERR0001 | Unable to decrypt RSA encrypted AES Key |
| NLMCERR0002 | Unable to decrypt AES encrypted payload |
| NLMCERR0003 | Unable to verify digital signature |
| NLMCERR0004 | Request not in proper format |

**Web Service Details**

All services will be implemented with above encryption approach.

1. **Aadhar Validation Request**
   1. Only OTP Validation in scope for INB
   2. INB will accept 12 digit Aadhar Number, API Request Reference Number (generated for every request), request initiated time to INB, residentConsent (Represents resident's explicit consent for accessing the resident's identity and address data from Aadhar system. Valid value is "Y")
   3. INB will
      1. Decrypt the payload
      2. Verify digital signature
      3. Capture request in DB with request time. Generate INB Reference number
      4. Reject the request, if residentConsent is not available or not having “Y”
      5. Reject the request, if request initiated time in the decrypted payload is greater than 3 minutes compared to current time
      6. Trigger EIS (storeData) Call to store the given Aadhar number to vault and get Aadhar Reference Number (ARN)
      7. INB will not store Aadhar number in DB. INB will capture ARN number in DB against the INB Reference number (generated while processing request at INB)
      8. Trigger OTP request to UIDAI via EIS (GenerateOTP) with ARN number
      9. INB will capture OTP Triggered time in DB against the INB Reference Number ( to validate 3 minutes)
   4. INB will respond with either success ( NLMC should display OTP page user) or failure ( in case of invalid Aadhar or connectivity issue)
   5. API Response will contain API Request Reference Number (shared in request), INB Reference Number, response initiated time, status, status description. NLMC to retail the “INB Reference number” shared as it will be used in subsequent services
   6. NLMC to reject any API response received after 3 minutes from the “response initiated time” available in decrypted payload

**Sample Request:**

**Payload fields** (payload will be encrypted)

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits(recommended-DDMMYYYY+9-digit sequence number) | y |
| data | String/12 digits (Aadhar number) | Y |
| residentConsent | String/1 digit | Y |
| requestInitiatedTime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr ":"22042024000000001”,

"payload":

{

" apirequestrefnbr ":"22042024000000001”,

"data":"123412341234",

"residentConsent":"Y",

"requestInitiatedTime":"22/04/2024 10:23:45"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Sample Response:**

**Payload fields** (payload will be encrypted):

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits | Y |
| inbrequestrefnbr | String/25 digits | Y |
| status | String/25 digits(success or failure) | Y |
| status\_desc | String/200 digits | Y |
| error\_code | String/25 digits | Y (if status is failure) |
| responseinitiatedtime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr ":"22042024000000001”,

"apistatus ":"success”,

"apierrrocode":"success”,

"payload":

{

"apirequestrefnbr ":"22042024000000001”,

"inbrequestrefnbr ":"avr22042024000000001”,

"status":"success”,

"status\_desc":"OTP Triggered to User”,

"error\_code":"”,

"responseinitiatedtime ":"22/04/2024 10:25:45"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Error codes (more error codes will be added later)**

|  |  |
| --- | --- |
| **Error Code** | **Description** |
| NLMCAVR0001 | Unable to process due technical or connectivity issues. |
| NLMCAVR0002 | Aadhar Validation Failure |
| NLMCAVR0003 | Resident Consent not provided |
| NLMCAVR0004 | Request rejected as INB received after 3 minutes of initiation time |

1. **Aadhar OTP Validation Request**
   1. Once user enters OTP in NLMC Page, NLMC to trigger the service for validation with API Request Reference number (generated for every request), INB Reference Number (returned in Aadhar Validation API Response) , request initiated time, OTP entered
   2. INB will
      1. Decrypt the payload
      2. Verify digital signature
      3. Update request in DB with request time based on the INB Reference number
      4. Reject the request, if request initiated time in the decrypted payload is greater than 3 minutes compared to current time
      5. Reject the request if request is coming after 3 minutes of OTP Generation.
      6. INB will fetch the ARN Number from INB DB based on the INB Reference Number
      7. INB will call “GetDetails” EIS API for OTP authentication with UIDAI using the ARN Number mapped for the Aadhar in the first request.
      8. INB will validate the EIS reference number in response against the reference number captured in DB before proceeding further
   3. If OTP validation is success, INB will success response and include “Name” returned from UIDAI in the response to NLMC
   4. If OTP validation is failure (business failure or connectivity issues), then INB will send failure response.
   5. INB will send following fields in response - API Request Reference number (came in request), INB Reference Number, Name returned from UIDAI (if status is success), Status, Status Description, response initiated time
   6. NLMC will validate the name returned from INB with their data before confirming success to end user for Aadhar Validation part of KYC

**Sample Request:**

**Payload fields** (payload will be encrypted)

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits(recommended-DDMMYYYY+9-digit sequence number) | y |
| data | String/6 digits (OTP entered by user) | Y |
| inbrequestrefnbr | String/25 digits( INB ref number shared in Aadhar Validation API Response) | Y |
| requestInitiatedTime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr":"22042024000000002”,

"payload":

{

"apirequestrefnbr":"22042024000000002”,

"inbrequestrefnbr":"avr22042024000000001”,

"data":"123456",

"requestInitiatedTime":"22/04/2024 10:27:45"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Sample Response:**

**Payload fields** (payload will be encrypted):

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits | Y |
| inbrequestrefnbr | String/25 digits | Y |
| status | String/25 digits(success or failure) | Y |
| name | String/200 digits | Y (if status is success) |
| status\_desc | String/200 digits | Y |
| error\_code | String/25 digits | Y (if status is failure) |
| responseinitiatedtime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key":"AXFFEREER",

"apirequestrefnbr":"22042024000000002”,

"apistatus":"success”,

"apierrrocode":"success”,

"payload":

{

"apirequestrefnbr":"22042024000000002”,

"inbrequestrefnbr":"aov22042024000000001”,

"status”: “success”,

"name":"Mr John Test”,

"status\_desc”: “Aadhar Validation Success”,

"error\_code":"”,

"responseinitiatedtime ":"22/04/2024 10:28:05"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Error codes (more error codes will be added later)**

|  |  |
| --- | --- |
| **Error Code** | **Description** |
| NLMCAOV0001 | Unable to process due technical or connectivity issues. |
| NLMCAOV0002 | Aadhar Validation Failure |
| NLMCAOV0003 | Request rejected as INB received after 3 minutes of initiation time |

1. **Aadhar OTP resend Request**

Can be used in case of failure (business or technical) in above OTP Validation request. Only one time this is allowed. INB need to retrigger new OTP via UIDAI for this.

* 1. NLMC to trigger the service for with API Request Reference number (generated for every request), INB Reference Number (returned in Aadhaar Validation Request API) , request initiated time, resend flag as yes
  2. INB will
     1. Decrypt the payload
     2. Verify digital signature
     3. Update request in DB based on the INB Reference number
     4. Reject the request, if request initiated time in the decrypted payload is greater than 3 minutes compared to current time
     5. INB will fetch the ARN Number from INB DB based on the INB Reference Number
     6. Trigger OTP request to UIDAI via EIS (GenerateOTP) with ARN number
     7. INB will capture OTP Triggered time in DB against the INB Reference Number ( to validate 3 minutes)
  3. INB will respond with either success ( NLMC should display OTP page user) or failure ( in case of invalid Aadhar or connectivity issue)
  4. API Response will contain API Request Reference Number (shared in request), INB Reference Number, response initiated time, status, status description
  5. NLMC to reject any API response received after 3 minutes from the “response initiated time” available in decrypted payload

**Sample Request:**

**Payload fields** (payload will be encrypted)

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits(recommended-DDMMYYYY+9-digit sequence number) | y |
| resendflag | String/3 digits (yes) | Y |
| inbrequestrefnbr | String/25 digits( INB ref number shared in Aadhar Validation API Response) | Y |
| requestInitiatedTime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr":"22042024000000003”,

"payload":

{

"apirequestrefnbr":"22042024000000003”,

"inbrequestrefnbr":"avr22042024000000001”,

"resendflag":"yes",

"requestInitiatedTime":"22/04/2024 10:28:45"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Sample Response:**

**Payload fields** (payload will be encrypted):

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits | Y |
| inbrequestrefnbr | String/25 digits | Y |
| status | String/25 digits(success or failure) | Y |
| status\_desc | String/200 digits | Y |
| error\_code | String/25 digits | Y (if status is failure) |
| responseinitiatedtime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key":"AXFFEREER",

"apirequestrefnbr":"22042024000000002”,

"apistatus":"success”,

"apierrrocode":"success”,

"payload":

{

"apirequestrefnbr":"22042024000000002”,

"inbrequestrefnbr":"aor22042024000000001”,

"status”: “success”,

"status\_desc”: “OTP Triggered to User”,

"error\_code":"”,

"responseinitiatedtime ":"22/04/2024 10:29:15"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Error codes (more error codes will be added later)**

|  |  |
| --- | --- |
| **Error Code** | **Description** |
| NLMCAOR0001 | Unable to process due technical or connectivity issues. |
| NLMCAOR0002 | Aadhar Validation Failure |
| NLMCAOR0003 | Request rejected as INB received after 3 minutes of initiation time |
| NLMCAOR0004 | OTP Attempts exceeded |

1. **PAN Validation Request**
   1. NLMC to trigger the service for with API Request Reference number (generated for every request), PAN, DOB (DD/MM/YYYY),Name (Name is combination of first name, middle name, last name or Name on card.) ,purpose of request, request initiated time

Note: Only for Department of Commercial Taxes – Father Name is mandatory. Hence, not included here.

* 1. INB will
     1. Decrypt the payload
     2. Verify digital signature
     3. Capture request in DB based on the INB Reference number
     4. Reject the request, if request initiated time in the decrypted payload is greater than 3 minutes compared to current time
     5. INB will call EIS service (TIN/PanInquiryAPIBackEnd)
     6. INB will capture OTP Triggered time in DB against the INB Reference Number ( to validate 3 minutes)
  2. INB will respond with either success or failure ( in case of business failure or connectivity issue)
  3. API Response will contain API Request Reference Number (shared in request), INB Reference Number, pan status, name matched status, dob matched status, seeding status , status, response initiated time
  4. NLMC to reject any API response received after 3 minutes from the “response initiated time” available in decrypted payload

|  |  |
| --- | --- |
| **File name in API response** | **Possible values and description** |
| pan\_status | E :EXISTING AND VALID  F : Marked as Fake  X : Marked as Deactivated  D :Deleted,  N : Record (PAN) Not Found in ITD Database/Invalid PAN  EA : Existing and Valid but event marked as Amalgamation in ITD database  EC : Existing and Valid but event marked as Acquisition in ITD database  ED : Existing and Valid but event marked as Death in ITD database  EI : Existing and Valid but event marked as Dissolution in ITD database  EL : Existing and Valid but event marked as Liquidated in ITD database  EM : Existing and Valid but event marked as Merger in ITD database  EP : Existing and Valid but event marked as Partition in ITD database  ES : Existing and Valid but event marked as Split in ITD database  EU : Existing and Valid but event marked as Under Liquidation in ITD database |
| name\_matched | Y-YES (If matched with Database), N - NO (If not matched with Database) [will be shared if pan\_status is E or E with event like EA) |
| dob\_matched | Y-YES (If matched with Database), N - NO (If not matched with Database) [will be shared if pan\_status is E or E with event like EA) |
| seeding\_status | Y-Operative PAN, R - Inoperative PAN, NA -For all non-Individual PANs [will be shared if pan\_status is E or E with event like EA) |

**Sample Request:**

**Payload fields** (payload will be encrypted)

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits(recommended-DDMMYYYY+9-digit sequence number) | y |
| data | String/10 digits (PAN Number) | Y |
| dob | String/10 digits(DD/MM/YYYY) | Y |
| name | String /85 digits(combination of first name, middle name, last name or Name on card) | Y |
| purpose | String/50 digits (only alphabets and space) | Y |
| requestInitiatedTime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr":"22042024000000004”,

"payload":

{

"apirequestrefnbr":"22042024000000004”,

"data":"ABCDE1234F”,

"dob":"10/10/9999",

"name":"mr john test",

"purpose ":"kyc check",

"requestInitiatedTime":"22/04/2024 10:35:45"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Sample Response:**

**Payload fields** (payload will be encrypted):

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits | Y |
| inbrequestrefnbr | String/25 digits | Y |
| status | String/25 digits (success or failure) | Y |
| pan\_status | String/2 digits | Y |
| name\_matched | String/1 digit | Y (if pan\_status is E) |
| dob\_matched | String/1 digit | Y (if pan\_status is E) |
| seeding\_status | String/1 digit | Y (if pan\_status is E) |
| error\_code | String/25 digits | Y (if status is failure) |
| responseinitiatedtime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key":"AXFFEREER",

"apirequestrefnbr":"22042024000000004”,

"apistatus":"success”,

"apierrrocode":"success”,

"payload":

{

"apirequestrefnbr":"22042024000000004”,

"inbrequestrefnbr":"pvr22042024000000001”,

"status”: “success”,

"pan\_status”: “E”,

"name\_matched”: “Y”,

"dob\_matched”: “Y”,

"seeding\_status”: “Y”,

"error\_code":"”,

"responseinitiatedtime ":"22/04/2024 10:36:15"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Error codes (more error codes will be added later)**

|  |  |
| --- | --- |
| **Error Code** | **Description** |
| NLMCPVR0001 | Unable to process due technical or connectivity issues. |
| NLMCPVR0002 | PAN Validation Failure |
| NLMCPVR0003 | Request rejected as INB received after 3 minutes of initiation time |

1. **GSTIN Validation Request**
   1. NLMC to trigger the service for with API Request Reference number (generated for every request), GSTIN Number, request initiated time
   2. INB will
      1. Decrypt the payload
      2. Verify digital signature
      3. Capture request in DB based on the INB Reference number
      4. Reject the request is GSTIN number is greater than 15 digits.
      5. Reject the request, if request initiated time in the decrypted payload is greater than 3 minutes compared to current time
      6. INB will call EIS service with GSTIN Number.
   3. INB will respond with either success or failure ( in case of business failure or connectivity issue)
   4. API Response will contain API Request Reference Number (shared in request), INB Reference Number, Legal Name returned from EIS, GSTIN Status, response initiated time, status, status description
   5. NLMC to reject any API response received after 3 minutes from the “response initiated time” available in decrypted payload

**Sample Request:**

**Payload fields** (payload will be encrypted)

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits(recommended-DDMMYYYY+9-digit sequence number) | y |
| data | GSTIN Number/15 digits | Y |
| requestInitiatedTime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key ":"AXFFEREER",

"apirequestrefnbr":"22042024000000005”,

"payload":

{

"apirequestrefnbr":"22042024000000005”,

"data":"123451234512345",

"requestInitiatedTime":"22/04/2024 10:48:45"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Sample Response:**

**Payload fields** (payload will be encrypted):

|  |  |  |
| --- | --- | --- |
| **Field Name** | **Data Type / Size** | **Mandatory** |
| apirequestrefnbr | String/25 digits | Y |
| inbrequestrefnbr | String/25 digits | Y |
| status | String/25 digits(success or failure) | Y |
| legal\_name | String/200 digits (Name of GST registered dealer) | Y (If status is success) |
| gstin\_status | String/25 digits | Y |
| registration\_date | String/25 digits | Y (If status is success) |
| cancellation\_date | String/25 digits | N |
| center\_jurisdiction | String/25 digits | Y (If status is success) |
| state\_ jurisdiction | String/25 digits | Y (If status is success) |
| nba\_accreditation | String/25 digits | Y (If status is success) |
| taxpayer\_type | String/25 digits | Y (If status is success) |
| status\_desc | String/200 digits | Y |
| error\_code | String/25 digits | Y (if status is failure) |
| responseinitiatedtime | Date Time (DD/MM/YYYY HH24:MM:SS) | Y |

{

"key":"AXFFEREER",

"apirequestrefnbr":"22042024000000005”,

"apistatus":"success”,

"apierrrocode":"success”,

"payload":

{

"apirequestrefnbr":"22042024000000005”,

"inbrequestrefnbr":"gvr22042024000000001”,

"status”: “success”,

"legal\_name”: “mr john test”,

"gstin\_status”: "",

"registration\_date”: "",

"cancellation\_date”: "",

"center\_jurisdiction”: "",

"state\_ jurisdiction”: "",

"nba\_accreditation”: "",

"taxpayer\_type”: "",

"status\_desc”: “GSTN Validation completed”,

"error\_code":"",

"responseinitiatedtime ":"22/04/2024 10:49:15"

},

"digitalsignature":"DDGRTRRT12323FRRR"

}

**Error codes (more error codes will be added later)**

|  |  |
| --- | --- |
| **Error Code** | **Description** |
| NLMCGVR0001 | Unable to process due technical or connectivity issues. |
| NLMCGVR0002 | GSTIN Validation Failure |
| NLMCGVR0003 | Request rejected as INB received after 3 minutes of initiation time |