**API Specification Document**

**voterIdVerification Service**

**Version 1.0**

**September 2021**

Copyright © 2019 IDFC FIRST Bank Limited. All Rights Reserved. This document contains sensitive & confidential information, and should not be disclosed, transmitted, duplicated, used in whole or part other than for its intended purpose and intended recipients.

**REVISION HISTORY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** | **Reviewer** |
| 21/09/2021 | 1.0 | Initial Base Document | Jay Soni | Mandar Shetye |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1. INTRODUCTION 4](#_Toc14805534)

[1.1 Definitions, Acronyms, and Abbreviations 6](#_Toc14805535)

[2. INTERFACE SERVICE DETAILS 6](#_Toc14805536)

[2.1 Error Codes: 6](#_Toc14805537)

[2.2 Sample Request Response: 7](#_Toc14805538)

[3. API Interface Testing 8](#_Toc14805539)

[4. Security Policy: SSL implementation 9](#_Toc14805540)

# INTRODUCTION

API will be used for verification of voter Id. The ESB mule service will have a direct integration with TotalKYC Gateway. ESB will send request to TotalKYC Gateway and they will be sending response after verifying the information.

**voterIdVerification:**

**UAT Endpoint URL Standalone MULE**: [**https://esbmuat.idfcfirstbank.com:31297/util-mgmt-exp/v1/voterIdVerification**](https://esbmuat.idfcfirstbank.com:31297/util-mgmt-exp/v1/voterIdVerification)

**Production URL -** [**https://esbm.idfcfirstbank.com/util-mgmt-exp/v1/voterIdVerification**](https://esbm.idfcfirstbank.com/util-mgmt-exp/v1/voterIdVerification%20)

**RTF UAT URL -** [**https://api.uat.internal.idfcfirstbank.com/util-mgmt-exp/v1/voterIdVerification**](https://api.uat.internal.idfcfirstbank.com/util-mgmt-exp/v1/voterIdVerification)

**Specifications:**

**HTTP Header's:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Filed Name | Mandatory/Non-Mandatory Value | Filed data- Type | Filed Probable Value | Filed Description |
| x-karza-key | Y | Header |  | Key |

**Request:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Filed Name | Mandatory/Non-Mandatory Value | | Filed data- Type | Filed Probable Value | Filed Description |
| msgHdr |  | |  |  |  |
| frm/id | | M | String | ABC | Consumer Name abbreviation, must be 3 alphabets only. (3rd party Name) |
| hdrFlds/msgId | | M | String | 12345 | Unique number for each request |
| hdrFlds/timestamp | | M | DateTimestamp | 2017-06-28T17:59:03 | YYYY-MM-DD T HH:MM:SS |
| msgBdy | |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| epicNumber | Y | String | "SHA4722088" | Voter’s EPIC Number to be authenticated. |

**Response:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| voterIdVerificationResponse | | | | | | |
| msgHdr | | | | | | |
| rslt | M | string |  | OK , ERROR |  | |
| error/cd | M | string |  | Error code | | Defined below |
| error/rsn | M | string |  | Error Reason | | Defined below |
| msgBdy | | | | | | |
| status-code | Y | String | “101” | Internal Status Code that denotes the status of the request. | |
| request\_id | Y | String | "f49749e6-26a8-425d-90e0-5a63023f4390" | Unique ID of the API request. | |
| result | N | Object |  | Response object for the given inputs. | |
| ps\_lat\_long | N | String | “0.0,0.0” | Lat Long for the polling booth applicable to the card holder | |
| rln\_name\_v1 | N | String | "विजयराज सामादारीया" | Name of Relative in vernacular language | |
| rln\_name\_v2 | N | String | “” | Name of Relative in vernacular language | |
| rln\_name\_v3 | N | String | “” | Name of Relative in vernacular language | |
| part\_no | N | String | “140” | Number of the part (location) in the constituency applicable to the card holder | |
| rln\_type | N | String | “F” | Relationship type: "F" = Father, "H" = Husband | |
| section\_no | N | String | “5” | Section of the constituency part applicable to the card holder | |
| id | N | String | "S131820140050293" | Unique ID of the card holder [st\_code+ ac\_no + part\_no + section\_no + slno\_inpart] | |
| epic\_no | N | String | “SHA4722088" | EPIC Voter ID number to be authenticated | |
| rln\_name | N | String | "Vijairaj Samdariya" | Name of relative in English | |
| district | N | String | "Mumbai City" | District of the Electoral Office | |
| last\_update | N | String | "11-10-2019" | Last date of update to the records against the given epic\_no in Government Records. | |
| state | N | String | "Maharashtra" | State of the registered Electoral Office | |
| ac\_no | N | String | "182" | Assembly Constituency Number applicable to the card holder | |
| slno\_inpart | N | String | "293" | Serial number of the card holder in the polling list in the applicable part | |
| ps\_name | N | String | "BrihanMumbai Mahanagarpalika, Worli Naka School, Ground Floor, Room No. 1, Dr. Annie Besant Road, Mumbai 400 018" | Polling Booth Address applicable for the card holder | |
| pc\_name | N | String | "Mumbai South" | Parliamentary Constituency applicable to the card holder | |
| house\_no | N | String | "1302" | House number of the residence of the card holder | |
| name | N | String | "Gaurav Vijairaj Samdariya" | Name of the card holder in English | |
| part\_name | N | String | "Dr. Annie Besant Road" | Name of the part (Location) in the constituency applicable to the card holder | |
| st\_code | N | String | "S13" | State Code | |
| gender | N | String | "M" | Gender of the card holder | |
| age | N | String | “31” | Age of the card holder in Years | |
| ac\_name | N | String | "Worli" | Assembly Constituency applicable to the card holder | |
| name\_v1 | N | String | "गौरव विजयराज सामादारीया" | Card holder’s name in vernacular language | |
| dob | N | String | "12-07-1987" | Date of Birth of the Voter Card holder as per EPIC records | |
| name\_v3 | N | String | “” | Card holder’s name in vernacular language | |
| name\_v2 | N | String | “” | Card holder’s name in vernacular language | |

Definitions, Acronyms, and Abbreviations

* **ESB** – Enterprise Service Bus
* **SMS Gateway** – SMS Gateway Team

# INTERFACE SERVICE DETAILS

## 2.1 Error Codes:

**Example of ESB Error Detail:**

|  |  |  |
| --- | --- | --- |
| **Error Type** | **MessageKey** | **Error Description** |
| ESB Technical Error | EXP\_400 | Bad Request |
| ESB Technical Error | EXP\_415 | Unsupported Media type |
| ESB Technical Error | EXP\_404 | Resource not found |
| ESB Technical Error | EXP\_405 | Method not allowed |
| ESB Technical Error | EXP\_503 | Connectivity Error |
| ESB Technical Error | EXP\_500 | Internal Server error |
| ESB Technical Error | EXP\_504 | HTTP Request timeout |

## 2.2 Sample Request Response:

**Success Scenario**:

|  |  |
| --- | --- |
| **REQUEST** | **RESPONSE** |
| {  "voterIdVerificationReq":{  "msgHdr":{  "frm":{  "id":"ABC"  },  "hdrFlds":{  "msgId":"1909P01",  "timestamp":"2020-09-19T10:43:23.162+05:30"  }  },  "msgBdy":{  "consent":"Y",  "epicNumber":"SHA4722088"  }  }  } | {  "voterIdVerificationResp":{  "msgHdr":{  "rslt":"OK"  },  "msgBdy":{  "result":{  "ps\_lat\_long":"0.0,0.0",  "rln\_name\_v1":"विजयराज सामादारीया",  "rln\_name\_v2":"",  "rln\_name\_v3":"",  "part\_no":"140",  "rln\_type":"F",  "section\_no":"5",  "id":"S131820140050293",  "epic\_no":"SHA4722088",  "rln\_name":"Vijairaj Samdariya",  "district":"Mumbai City",  "last\_update":"11-10-2019",  "state":"Maharashtra",  "ac\_no":"182",  "slno\_inpart":"293",  "ps\_name":"BrihanMumbai Mahanagarpalika, Worli Naka School, Ground Floor, Room No. 1, Dr. Annie Besant Road, Mumbai 400 018",  "pc\_name":"Mumbai South",  "house\_no":"1302",  "name":"Gaurav Vijairaj Samdariya",  "part\_name":"Dr. Annie Besant Road",  "st\_code":"S13",  "gender":"M",  "age":31,  "ac\_name":"Worli",  "name\_v1":"गौरव विजयराज सामादारीया",  "dob":"12-07-1987",  "name\_v3":"",  "name\_v2":""  },  "request\_id":"f49749e6-26a8-425d-90e0-5a63023f4390",  "status-code":"101"  }  }  } |

**Failure Scenario:**

|  |  |
| --- | --- |
| **Request** | **Response** |
| **ESB Error:**  {  "voterIdVerificationReq":{  "msgHdr":{  "frm":{  "id":"ABC"  },  "hdrFlds":{  "msgId":"1909P01",  "timestamp":"2020-09-19T10:43:23.162+05:30"  }  },  "msgBdy":{  "consent":"Y",  "epicNumber":"SHA4722088"  }  }  } | {  "voterIdVerificationResp":{  "msgHdr":{  "rslt":"ERROR",  "error":[  {  "cd":"SYS\_500",  "rsn":"Internal Server Error",  "srvc":{  "nm":"krz-util-sys",  "cntxt":"krz-util-sys",  "actn":{  "paradigm":"Reply",  "nm":"voterIdVerification",  "vrsn":"1.0.0"  }  }  }  ]  },  "msgBdy":{    }  }  } |

s

# API Interface Testing (Third-Party Integration)

This API can be tested using curl command.

**Syntax:**

curl -H "Content-Type: application/json" -X POST -d '{Add JSON Request}'  <API\_URL>  --cert <cert.pem> --key <privkey.pem> -k

**Note: --cert=Public certificate (Client Certificate) --key=Private Key (Client Private Key).**

# Security Policy: SSL implementation

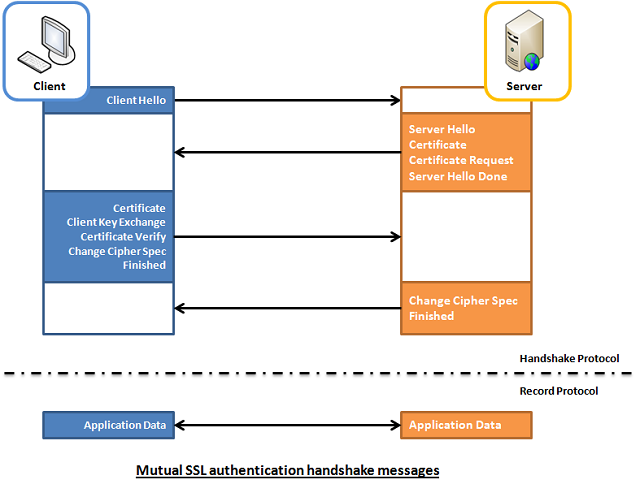
**SSL Authentication:**

**2-way SSL authentication**

**Mutual SSL Authentication (server 🡪 client)**

Whereas in mutual SSL authentication, both client and server authenticate each other through the digital certificate so that both parties are assured of the others' identity. In this aspect, both client and server use **12** handshake messages to establish the encrypted channel prior to message exchanging.

1. Client sends ClientHello message proposing SSL options.
2. Server responds with ServerHello message selecting the SSL options.
3. Server sends Certificate message, which contains the server's certificate.
4. Server requests client's certificate in CertificateRequest message, so that the connection can be mutually authenticated.
5. Server concludes its part of the negotiation with ServerHelloDone message.
6. Client responds with Certificate message, which contains the client's certificate.
7. Client sends session key information (encrypted with server's public key) in ClientKeyExchangemessage.
8. Client sends a CertificateVerify message to let the server know it owns the sent certificate.
9. Client sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.
10. Client sends finished message to let the server check the newly activated options.
11. Server sends ChangeCipherSpec message to activate the negotiated options for all future messages it will send.
12. Server sends finished message to let the client check the newly activated options.



**Oauth 2.0 – Process to generate bearer tokens**

ABC Client ID UAT:

cb76b001-8a9a-4f60-aa2d-b648fcc63e1f

s**Step 1: Generate JWT Token**

1. Go to <https://jwt.io> and select RS256 as algo
2. Enter below to header section (Copy as is)

**{**

**"alg": "RS256",**

**"typ": "JWT",**

**"kid":"Sl-UGgjxNyh3ctHsBnnDGliz4Z5a4TbzEG0gWG3lmVk"**

**}**

1. Enter below into payload section (change jti to unique value, sub and iss is client id mentioned above, aud keep as is and exp is the expiry of the JWT token that will be generated)

**{**

**"jti":"1623863273000",**

**"sub":"cb76b001-8a9a-4f60-aa2d-b648fcc63e1f",**

**"iss":"cb76b001-8a9a-4f60-aa2d-b648fcc63e1f",**

**"aud":"https://app.uat-opt.idfcfirstbank.com/platform/oauth/oauth2/token",**

**"exp":1654080528**

**}**

1. Copy the public and private key into the signature section
2. Copy the jwt from left side panel

**Step 2: Generate Bearer Token**

1. Use reqbin.com or Postman with below settings
2. Method = POST and URL = <https://app.uat-opt.idfcfirstbank.com/platform/oauth/oauth2/token>
3. Use below headers

**Content-Type: application/x-www-form-urlencoded**

**Accept: application/json**

1. Copy below to content

**grant\_type=client\_credentials**

**scope=generic-ovd-verify**

**client\_id=cb76b001-8a9a-4f60-aa2d-b648fcc63e1f**

**client\_assertion\_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer**

**client\_assertion=<<jwt token from step 1>>**

1. Click on Send. You will get the bearer token which can be used in API’s Authorization header
2. Sample response –

{

"access\_token": "VMJ0EyZ0XoB8o-

ADfRQTOaCmX\_Nq9g2CtWRH\_oVsZ7U.SwWVjcboTVYhnJOti00I4IHKZ8MwHiKRT-nbuT8c3FI",

"expires\_in": 1799,

"scope": "si-mgmt-createCBS-SI",

"token\_type": "bearer"

}

Available Scopes (multiple scopes can be mentioned separated by space in above request):

**generic-ovd-verify**

**partner-kyc-eligiblemodes**

**partner-kyc-ckyc**

**partner-loan-create**

**partner-bank-loan**