Data Fied Def\_Req

| S.No. | Name | Type | Description |
| --- | --- | --- | --- |
| 1 | individualId\* | >UIN generated should be of the length defined by the ADMIN. In absence of configured length policy, UIN generated should be of 12 digits >VID generated should contain the number of digits as configured by the ADMIN In absence of ADMIN configured length, VID generated should have 16 digits | UIN or Virtual ID |
| 2 | **transactionID\*** | Alphanumeric(10) | AUA/Internal Module specific transaction Identifier - To map Request and Response transaction |
| 3 | version\* | NA | Version of the Authentication API |
| 4 | **requestTime\*** | DateTime - ISO 8601 | Timestamp at the time of request. This is in format “YYYY-MM- DDThh:mm:ss” (derived from ISO 8601).  Time standard - UTC |
| 5 | **individualIdType** | Character(1) | Type of request  · “U” –attribute value shall contain UIN number (this is the default option). If “type” attribute is missing, it is assumed that “UIN Type” field contains a valid UIN.  · “V” –attribute shall contain a Virtual ID. |
| 6 | **bio\*** | Character(1) | Valid values are “y” or “n”. If the value is “y” then at least one attribute of element “bio” should be used in authentication. |
| 7 | deviceCode\* | NA | Device Code |
| 8 | deviceProviderID\* | NA | Device Model ID |
| 9 | bioType\* | NA | a comma separated list of biometrics used. Valid values that can be used in this comma separated list are “FMR”, “FIR”, “IIR” and “FID”. If “FMR” is part of the list, then at least one “Bio” element with type FMR should be used. Similarly, if “FIR” or “IIR” or “FID” are part of the list, then at least one “Bio” element with those types must be used. |
| 10 | bioValue |  | FMR- The biometric data is of type “Fingerprint Minutiae Record”. This data is in ISO minutiae format with no proprietary extensions allowed.  FIR- The biometric data is of type “Fingerprint Image Record”. The data is a fingerprint image packaged in ISO 19794-4 format, which could contain a lossy compressed image of type Jpeg2000.  IIR- The biometric data is of type “Iris Image Record”. The data is an iris image packaged in ISO 19794-6 format, which could contain a lossy compressed image having type Jpeg2000.  FID - The biometric data is of type “Face Image Data”. The data is face image packaged in ISO 19794-5 format, which could contain a lossy compressed image having type Jpeg2000. Only one face image need to be there along with another modality. Usage of face alone as biometric modality will result in error |
| 11 | bioSubType\* | NA | Valid values are   |  | | --- | | LEFT\_IRIS | | RIGHT\_IRIS | | LEFT\_INDEX | | LEFT\_LITTLE | | LEFT\_MIDDLE | | LEFT\_RING | | LEFT\_THUMB | | RIGHT\_INDEX | | RIGHT\_LITTLE | | RIGHT\_MIDDLE | | RIGHT\_RING | | RIGHT\_THUMB | | FACE | | UNKNOWN | |

|  |
| --- |
| Notes: |
| * \* denotes mandatory * The current data definition is for fingerprints only, Based on detailing iris and face modalities the data definition pertaining to those modalities will be updated |

Data Fied Def\_Res

|  |  |  |  |
| --- | --- | --- | --- |
| S.No. | Name | Type | Description |
|  | Response Section | | |
| 1 | **status** | Character(1) | Result of Authentication request ‘y’ or ‘n’. |
| 2 | **transactionID** | NA | same as Request |
| **3** | **responseTime** | DateTime - ISO 8601 | Time stamp of response. This is in format “YYYY-MM- DDThh:mm:ss” (derived from ISO 8601).  Time standard - UTC |
| 4 | errors | NA | Error codes and Error Messages as defined in the Error Messages Document |
| 5 | staticToken | NA | This is the Partner and UIN specific token generated and sent in the response |