

Offline Aadhaar Data Verification Service

Offline Aadhaar Data Verification Service

Definition: It is a secure sharable document which can be used by any Aadhaar number holder for offline verification of Identification.

A resident desirous of using this facility shall generate his/her digitally signed Aadhaar details by accessing UIDAI resident portal. These details will be generated by the Aadhaar number holder which will contain Name, Address, Photo, Gender, DOB, registered Phone Number (hashed) and registered Email Address (hashed). Apart from Name and Address as mandatory details in digitally signed XML, Aadhaar number holder will always have the option to choose from other five demographic details which he/she may want to share with any service provider using the XML. It will provide Offline Aadhaar Verification facility to service providers without the need to collect or store Aadhaar number.

Generation of Offline Aadhaar

The process of generating Offline Aadhaar is explained below:

- a) Go to URL → <https://resident.uidai.gov.in/offlineaadhaar>
- b) Enter 'Aadhaar Number' or 'VID' and mentioned 'Security Code' in screen, then click on 'Send OTP'. The OTP will be sent to the registered Mobile number for the given Aadhaar number or VID. Enter the OTP received and click on 'Submit' button
- c) On the next screen, enter the 'Name', 'Pin Code' as registered in Aadhaar and mentioned 'Security Code' in screen and click on 'Verify' button. This will validate the 'Name' and 'Pin Code' for the given Aadhaar number or VID. Upon successful validation, it will redirect to next screen, else it will redirect to page mentioned in step 'b' with error message as "Please re-check your details, data does not match our records".
- d) In next step, after successful validation,
 - i. Select the required details which you want to download by clicking the radio button.
 - ii. Enter the desired 'Share Code' for the ZIP file in the provided field with required parameters as indicated in screen
 - iii. Enter the 'Security Code' and press 'Submit' button
- e) The Zip file containing the digitally signed XML will be downloaded to device wherein the above mentioned steps have been performed. Extract the zip

file using the password as specified in previous step and save the XML file in the desired location

Users of this Offline Aadhaar Data Verification Service

Any Aadhaar number holder who desires to establish his/her identity to any service provider using digitally signed XML downloaded from UIDAI website can be a user of this service. The service provider should have provisions of providing this Offline Aadhaar Data Verification Service at their facility and do the offline verification (as described below)

Sharing of Aadhaar XML file with the service provider

Residents are free to share this ZIP file along with the Password (Share Code) to the service provider as per their mutual convenience

Use of Offline Aadhaar Data Verification Service by Service Providers

The process of Offline Aadhaar Data Verification by Service Provider is:

- a) Once service provider obtains the ZIP file, it extracts the XML file using the password (share code) provided by the resident
- b) The XML file will contain the demographic details such as Name, DOB, Gender and Address in plain text. Photo is base 64 encoded which can be rendered directly using any utility or plain HTML page. Email Address and Mobile number are one-way hashed.
- c) Service Provider has to collect Email Address and Mobile number from residents and perform below operations in order to validate the hash:

Mobile Number:

Hashing logic: $\text{Sha256}(\text{Sha256}(\text{Mobile} + \text{ShareCode})) * \text{number of times of last digit of mobile number}$

Example:

Mobile number: 9800000002

Share Code: Abc@123

$\text{Sha256}(\text{Sha256}(9800000002 + \text{Abc@123})) * 2$

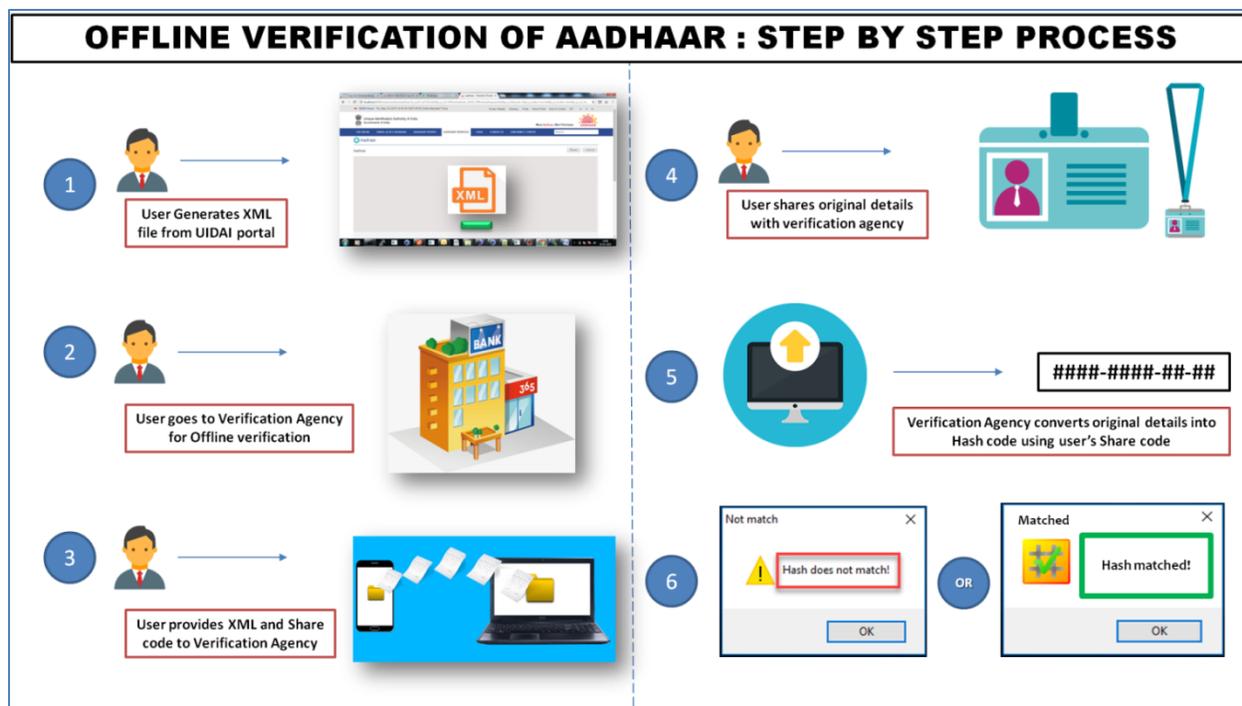
In case of mobile number ends with Zero (9800000000) it will be hashed one time.

$\text{Sha256}(\text{Sha256}(9800000000 + \text{Abc@123})) * 1$

Email Address:

Hashing Logic: This is a simple SHA256 hash of the email without any salt

- d) Entire XML is digitally signed and Service Provider can validate the XML file using the signature and public key attached in the XML



Sharing of Aadhaar XML file to other entities by the Service Provider

Service Providers shall not share, publish or display either Share Code or XML file or its contents with anyone else. Any non-compliance of these actions shall invite actions under Sections 17 and 25 of The Aadhaar (Authentication) Regulation, 2016, Sections 4 and 6 of The Aadhaar (Sharing of Information) Regulation, 2016 and Sections 29(2), 29 (3) and 37 of The Aadhaar Act, 2016.

Difference between other identification documents produced offline by residents and Aadhaar XML document

Identity verification can simply be accomplished by providing an identity document like PAN card, Passport etc to the service provider. However, all these documents, which may be used for identification can still be forged and faked which may or may not be possible to verify offline instantaneously. The document verifier has no technological means to verify the authenticity of the document or the information it contains and has to trust the document producer. Whereas, the XML file generated by the Aadhaar number holder using Offline Aadhaar Data Verification Service is digitally signed document using UIDAI digital signature. Thus, the service provider can verify the demographic contents of the file and certify it to be authentic when doing the offline verification