UIDAI HACKATHON 2021

Target Audience: Students of Engineering Colleges

Theme 1: Authentication Reimagined

Indian citizens are witnessing a period of hypergrowth in the Smartphone domain. 4G based Smartphone subscription in India is set to grow from 680 million in 2020 to 830 million in 2026, increasing at a CAGR of 3 percent. With the introduction of 5G, it is expected that around 26 million subscribers will migrate to this new technology by the end of 2026. Smartphones will become an important device for every resident and would be the de facto instrument to interface with **Digital India**.

UIDAI intends to leverage this behavioral change in the life of a citizen and would like to reimagine the authentication and identity platform. In addition, these changes intend to improve the usability, security, and privacy of Aadhaar Authentication.

In each hackathon challenge below, you are expected to develop a resident application, a verifier application and demonstrate the communication between them to solve the hackathon challenge.

- **Resident Application**. An application running on the resident personal device, which can avail authentication products of the UIDAI. This application facilitates secure communication between UIDAI and residents without any intermediaries.
- **Verifier Application**. This is a third party application, using the Aadhaar services to validate the claims of residents. Authentication User Agencies (AUA) applications are in this category, though it is not limited to AUA applications and could include applications from third parties (who are not allowed to have access to the Aadhaar Number). Sensitive data on such an application should be protected and minimized.

UIDAI will provide some sample application as a starting point for the hackathon:

- ○ A sample verifier app/code is available for participants.
- ○ This sample code has Aadhaar Auth APIs using UIDAI staging sandbox. [1]

UIDAI will provide API endpoint specifications and access to the staging sandbox to understand how to interact with the UIDAI endpoints.

Innovative applications of UIDAI authentication products

In this challenge, you are required to design and develop an innovative real-world application using one or more of the authentication services provided by UIDAI. Examples of a real world application include, but are definitely not limited to:

Airport / Stadium / Railway Station / Hotel Check-in Application: How could we use Aadhaar services to create an application for smooth check-in to a Airport/Railway Station/Hotel etc ? Please remember that the Aadhaar number should not be shared with the verifier application. In addition, the verifier application should be assumed to have no access to UIDAI servers. The application should work offline and provide a sub-second end-to-end response time.

Aadhaar backed Video KYC / Liveness Certificate: Suppose you wish to open a bank account or get a liveness certificate from a bank through a video call with a bank officer. Build a system that can help the bank (verifier) establish your identity (resident) without accessing the biometric authentication platforms of UIDAI. In particular, the resident shares the offline eKYC document (avbl in XML format) with the verifying agency for validation. The verifier will use the photo taken through the video call and match it against the photo available in the eKYC document. The verifier application can use the headless face authentication APK of UIDAI to validate the eKYC document in a completely offline (not connected to UIDAI backend systems) manner for genuineness and authenticity using face match technology.

Usage of Aadhaar as an additional factor in a high value third party transaction: How can I try to connect.

To edit offline, turn on offline sync. We use Aadhaar to improve the trust in a third party transaction. Can we get a “token” (digitally signed authentication response) from an Aadhaar authentication from online face authentication on the resident mobile and later use this token as an additional (second) factor of authentication in a third party application. As always, Aadhaar numbers should not be exposed to third party applications.

Achieving 100% authentication success in Rural India: Implement fingerprint (may use OTP in the hackathon) as the primary authentication modality. Use face authentication for residents for whom fingerprint(OTP) does not work. Use offline face authentication when network connectivity is not available. As always, Aadhaar number need not be exposed to the verifier application

Available UIDAI authentication Services/APK

- **Aadhaar Authentication API:**
  - https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf

- **Aadhaar eKYC API:**
  - https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_5.pdf
- **Virtual Identity (VID) API**: VID is a 16 digit number generated for a limited duration that can be used instead of the Aadhaar number for various authentication services. The use of VID removes the need for sharing Aadhaar with various service providers, thereby preserving the privacy of the resident.
- **Offline Electronic Know Your Customer (eKYC) API**: A resident can download an offline eKYC document (in XML format) from the UIDAI APIs/portals after OTP authentication. The eKYC can later be shared with the verifier to establish identity.
- **Aadhaar Face Authentication APK:** Aadhaar provides a secure, packaged APK for both online and offline face matching**.**