Registered Devices for Authentication Applications Dec 22, 2015

Unique Identification Authority of India

Public Devices

- **Public Devices**: During authentication, encryption of Personal Identity Block (pid) including biometrics is happening at desktop / PoS OS level, not at device level
- **Secure Authentication can be achieved through**:
  - Devices used in Assisted Mode viz. through appropriate trained/certified operator
  - Signed application with appropriate App Monitoring Services
  - Usage of Multi Factor Authentication and Auditing of devices from Service Provider end
  - Maintaining a dashboard at service provider side for monitoring the devices with unique identifiers

AADHAAR

Public Devices

- **Challenges**
  - This is prone to **replay attack**
  - It is difficult to set the unique identity of the device
  - It is not safe to use in self mode like in Jeevan Pramaan application
  - Limitation in covering large number of devices for authentication

AADHAAR

Registered Devices

Registered Devices Offer:

- Unique identifier for every physical sensor device
- Data Encryption at the device level
- Elimination of stored biometrics and misuse of resident biometric data on the host side where client data is transmitted to UIDAI
- Acceptance of authentication requests only from the devices that are registered with UIDAI

AADHAAR

Registered Devices - Overview

1. Device registration/reset includes application and hardware level specifications
2. Each manufacturer will register each device with UIDAI
3. With device registration by UIDAI, every auth transaction can be traced to a specific device
4. Implementation of registered devices is taken up in a phased manner

AADHAAR

REGISTER and RESET Process

REGISTER

- Manufacturer procures public key from CA, shares public key with UIDAI, and get a “Manufacturer Key” issued by UDIAI
- Manufacture hardware with secure storage and embedded firmware.
  - a. Firmware having security and biometric processing capability
  - b. Embed a unique PhysicalID, ModelID, Manufacturer Key.
- Certify model as a compliant registered device and other accuracy related certifications
- Register every individual physical device unit using the secure registration API before field distribution and use.

RESET

- Device may be reset many times during itz life time.
- Administrator of the device forcing a reset due to an encryption error.
- When UIDAI server gives an explicit error code as part of authentication API indicating that a reset is mandatory due to UDIAI key rotation policy.
- Reset the device using the API

AADHAAR

Registered Devices - Timelines

Activity	Status / Timeline
RFI	Published on Feb 2015; Responses were reviewed in Mar 2015
EOI	Published on Apr 2015 – 7 Responses Received, 4 vendors shortlisted
PoC	○ Back End development and initial testing with Vendors finished for all Modules of Register, Reset and Auth (Pre-Alpha) ○ A prototype is ready and can be put under extensive testing ○ PoC is completed and results are being analyzed.
Device Specification Finalization, Vendor Workshop	By Jan 2016
STQC Device Certification	By Feb 2016

Thank You

AADHAAR