Guidance to applicant

for

Registered Devices for

UID Application

STQC - IT Services
STQC Directorate, Ministry of Electronics & Information Technology, Electronics
Niketan, 6 CGO Complex, Lodi Road,
New Delhi – 110003

April 2017
**Testing & Certification of “Registered Devices for UID Applications”**

1. **Services Offered:**

2. **Client:**
   Vendors (Manufacturers/ suppliers) of Registered Devices (Discrete Fingerprint, Discrete iris & Integrated Iris/FPS)

3. **Purpose & Objectives of Testing & Certification:**
   The key aim of testing & certification is to ensure that the Device Under Test (DUT) complies with the security requirements, relevant standards specifications including specifications released by UIDAI for Aadhaar based applications.
   The objectives are to verify that:
   a) To verify that the DUT meets UIDAI registered device specification achieving L0 or L1 compliance.
   b) To verify that the DUT meets all environmental, safety and accuracy requirements as per STQC specification.
   c) Provide opportunity for Vendors to understand defects/ conformance and rectification of the same.
   To grant certification and provide assurance to users of devices that the certified product meets UIDAI requirements comprehensively i.e security, accuracy (FRR) & quality for the purpose of Aadhaar based Authentication.

4. **Scope of Work:**
   The scope includes testing & certification of the following Devices that include:
   a) Discrete Fingerprint Scanner
   b) Discrete Iris Camera
   c) Integrated Iris cameras
   d) Integrated FP devices (in near future)
   The Devices will be tested for the following:
   - The devices which already gone through the accuracy and reliability testing by the ETDC Mohali Lab will now be tested for compliance to the UIDAI registered device specification.
   - Provisional certification will be valid for the period Mar 15th 2017 to December 2017
• The devices used for delivering various UID services including authentication services are capable of delivering the outputs as specified by the UIDAI and meet the UIDAI registered device requirements specified by UIDAI for Provisional Certificate.
• The device should be able to integrate with software application for Authentication using “Aadhaar Authentication API 2.0 (Revision 1)”.
• June 2017 onwards final certification for registered devices shall be initiated. All the security related testing as per UIDAI registered device specification or any other test envisaged as necessary by STQC (for compliance to the registered device specification) shall be carried out before the issue of final certification. This certificate shall be valid for a period of three years or as per the directions from UIDAI.

The following types of tests will be conducted on the Registered Device as per specified requirements:
• Compliance statement by client for meeting Registered Devices criteria published by UIDAI
• The vendor shall ensure the UIDAI requirements have been addressed, and provide traceability document from UIDAI requirement to solution architecture. Operational demo by the vendor.
• Execution of test cases with tools & scripts provided by UIDAI
• Security tests listed as per appendix
• Test case execution by vendors in presence of UIDAI & STQC engineers. Vendor to provide test points & tools / jig as required.

For the purpose of provisional certification, solution architecture, functional testing and self-certification are requirements. As regards the security testing, the solution expected to pass all security test, however only a subset of the tests will be executed at this time.

Note: In order to verify compliance to the device security specifications and other key requirements one or more of the followings will be used:
• Testing may be conducted in the STQC laboratory.
• External test laboratory/ client’s test facility may be used to conduct the testing (where test facilities are not available with STQC).
• Compliance may be verified by demonstration(s) of testing using client’s test facilities.
• Compliance may be verified based on the test reports &/or certifications obtained by the client (subject to verification of test results on sample basis).

To carry out testing following shall be arranged:
• Test Tool / Software would be provided by UIDAI.
• Vendor to provide test points / probes tools & techniques to demonstrate of compliance along with an undertaking for meeting the requirement.
• L1 certification will include additional testing beyond that which is required for L0 certification.

5. Inputs Required by STQC for Provisional Certificate:
Access to the followings information & facilities/ systems to undertake testing of Registered Devices will be required by STQC:
• UID Requirements – Registered device specifications, API Documentation
• Device Documentation – RD Service Documentation, Management Client Documentation, Management Server documentations,
• Authentication client for testing purpose only.
• FRR Testing Report
• ETDC Mohali Test Report
• Test environment for testing of specialized security parameters (if required)
• Internal test reports of client
• Arrangement to witness the testing at client’s facility, in case the in-house facility for the same is not available with STQC

Vendors would need to be directly providing the documentation to STQC and as per the certification needs provide additional information/Test results.

6. Activities to be performed:
6.1 Testing Activities:
6.1.1 Study & Understanding security of Registered Devices
6.1.2 Test Planning & Preparation
6.1.3 Test Execution
6.1.4 Test Report Preparation
6.2 Certification Activities:
6.2.1 Analysis of test results
6.2.2 Verify compliance to evaluation criteria
6.2.3 Issue of Certificate (if evaluation criteria is met)

7. Deliverables:
The following deliverables will be provided to the client:
• Security Test Report
• Certificate, subject to fulfillment of evaluation criteria
8. **Test & Certification Schedule:**
   - It will take about 4-6 weeks to complete the testing and certification after required inputs have been provided by the client to STQC for final certification. Provisional certification should become available within one working week after submission.

9. **Terms & Conditions:**
   - The client shall arrange for DUT and support environment at STQC test lab where testing will be undertaken.
   - In order to complete the testing, as per schedule, client shall ensure readiness of test related documentation and timely availability of the required information.
   - STQC shall ensure timely completion of test activities as per plan and submit the deliverables.
1. AADHAAR REGISTERED DEVICES TECHNICAL SPECIFICATION - VERSION 2.0 (REVISION 1) http://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_1.pdf
2. AADHAR AUTHENTICATION API SPECIFICATION –VERSION 2.0 (REVISION 1) http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0_1.pdf
Certification of Registered Devices

<table>
<thead>
<tr>
<th>Application fee</th>
<th>Rs. 10,000/-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit/ Testing, Evaluation &amp; Certification fee</td>
<td>L0 Rs. 75,000/-</td>
</tr>
<tr>
<td></td>
<td>L1 Rs. 1,50,000/-</td>
</tr>
</tbody>
</table>

**Additional Certificate Charges**: Rs.10,000/- for each additional copy of certificate

*Note: In case of technical changes re-audit will be done.*

*Note: Service Tax and other Charges shall be charged extra as per applicable rates*

*Note: If change of scope re-audit will be done as per the change in extent and dependencies.*
Overview:

This document outlines the requirements and testing methodology for the provisional certification of registered devices.

Any sensor that has been approved by STQC for authentication under the previous certification may participate in the provisional certification scheme. This will result in the issuance of a provisional certificate having a validity till Dec 31st 2017.

Sensors, that are in the process of STQC certification may continue the existing certification process. In parallel, they may apply for provisional RD service certification. Both current STQC certification for the device under the existing scheme for authentication device certification, as well as provisional RD service certification is required to allow deployments in the field.

All authentication end user devices (for e.g. POS terminals) must possess RD Service provisional certification. Under this scheme, biometric sensor vendor could apply for RD service and supply provisionally certified sensor and service to the ecosystem. End User device vendors who use an RD service certified by sensor vendor, need not apply for RD service provisional certification along with the sensor certified by STQC. In all other cases, end user device vendors need to apply for RD Service certification.

Provisional certification will be performed in the premises of the UIDAI Technology Centre at Bangalore from Apr 17th to June 1st 2017. STQC personnel will monitor the provisional certification tests, and STQC will issue provisional certificates based on the reports generated during testing.

Device vendors will be required to submit three test samples for Registered Device Testing along with the application form and requisite charges.

Solution Architecture:
System architecture describes the architecture of the proposed registered device solution including all hardware and software components. Providing detailed solution architecture is mandatory during applying for certification (Add diagrams wherever is applicable). Please be descriptive as lack of complete information may delay the certification process.

a. Describe solution architecture and explain why it is compliant with the L0/L1 registered device specifications
   ■ Show that it is not possible to insert a (stored) biometric into the RD service and get it signed and encrypted
   ■ Show that it is not possible to extract the private key of the registered device

b. L1 Compliance:
Show how the biometrics are signed and encrypted within the trusted execution environment. (Firmware or Hardware Solution)

Provide internationally relevant certifications for protection of the keystore in the trusted execution environment

Provide methodology and tools to allow certifying agency to verify the L1 compliance for final certification

c. L0 Compliance:

Describe the software keystore implementation

- Standard keystore used (Android, CSP, Java keystore, P12 etc.)
- Custom keystore used
  - Where is the file located?
  - File permission details
  - Keystore access rights
  - Password generation logic
  - Password strength
  - Dynamic ability in password

d. Describe the sequence diagram for the “init” function implementation. Register, key rotate, update RD service, update UIDAI public key

The details should contain all the hop points (function names and the accessors and the file names of the binary should be used as the module name) till it reaches the sensor
Sample Sequence Diagram. - Auto generated
e. Describe the sequence diagram for “capture” function implementation
   - Submit code for RD service and capture_sign_encrypt service (this can be part of point e above).
   - Quality check, Preview, Capture Sequence etc.
   - The details should contain all the hop points (function names and the accessors and the file names of the binary should be used as the module name) till it reaches the sensor.
   - Confirm that capture_sign_encrypt service and key management is implemented as native compiled code

f. Registered Device (RD) Service Discovery
   - Discovery of the RD service
   - Handling multiple RD services on the same host
   - Allow multiple applications talk to the same RD service

g. Management Server
   - Management Server Architecture
   - Deployment and security architecture
   - HSM security in Management Server

The proposed solution architecture should include a completed traceability matrix to identify how the requirements are met by the solution. A spreadsheet detailing the traceability matrix is as under:

<table>
<thead>
<tr>
<th>S.No</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Entity applying for RD service certification</td>
</tr>
<tr>
<td>2</td>
<td>Sensor Models for RD service certification is requested (RD service may support multiple sensors)</td>
</tr>
<tr>
<td>3</td>
<td>Name of entity which applied for original sensor certification</td>
</tr>
<tr>
<td>4</td>
<td>Operating System(s) for which RD service certification is required (There will be separate installable for each OS)</td>
</tr>
<tr>
<td>5</td>
<td>Modality (Fingerprint / Iris)</td>
</tr>
<tr>
<td>6</td>
<td>Level of compliance claimed (L0/L1)</td>
</tr>
<tr>
<td>7</td>
<td>Diagram showing the solution architecture and all its components</td>
</tr>
<tr>
<td>8</td>
<td>Show that it is not possible to insert a (stored) biometric into the RD service and get it signed and encrypted</td>
</tr>
<tr>
<td>9</td>
<td>Show that it is not possible to extract the private key of the registered device</td>
</tr>
<tr>
<td>10</td>
<td>Submit source code for RD service and capture, sign and encrypt service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>For L1 Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>For L0 Standard Keystore</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>22</td>
</tr>
<tr>
<td>For L0 Custom Keystore Implementation</td>
</tr>
<tr>
<td>23</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>25</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>27</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>29</td>
</tr>
<tr>
<td>Sequence Diagram for &quot;init&quot; Function</td>
</tr>
<tr>
<td>30</td>
</tr>
<tr>
<td>31</td>
</tr>
<tr>
<td>32</td>
</tr>
<tr>
<td>33</td>
</tr>
<tr>
<td>Sequence Diagram for &quot;capture&quot; Function</td>
</tr>
<tr>
<td>34</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>36</td>
</tr>
<tr>
<td>RD Service Discovery</td>
</tr>
<tr>
<td>37</td>
</tr>
<tr>
<td>38</td>
</tr>
<tr>
<td>39</td>
</tr>
<tr>
<td>Management Server</td>
</tr>
<tr>
<td>40</td>
</tr>
<tr>
<td>41</td>
</tr>
<tr>
<td>42</td>
</tr>
</tbody>
</table>
**Declarations (L0 & L1 both):**

The device provider will need to make the following declarations

- It is certified that there is no debug or backdoor mechanism exist to insert a biometric into the RD service and get it signed and encrypted by the RD service.

- It is certified there is no debug or backdoor mechanism to extract the private key from the RD service and no known bugs/exploits/vulnerabilities/configurations in the OS or any other components that the RD services uses from where an attacker could extract the private key at the time of certification, especially for L0 devices.

- It is certified that the Device provider will actively watch for any known attacks or exploits or vulnerabilities that could help an attacker extract the keys and work towards patching the same.

- It is certified that Device provider private key is secured using an HSM and appropriate access control and monitoring mechanisms are in place within the management server environment to protect access to production machines.

- I understand that at any point of time, if my device-application is found non-conforming to any of the points declared and above, my certification may be revoked without any justification and I shall be abiding by all applicable legal consequences as per Govt. rules and regulations.

**For L1 Devices only:**

- It is certified device signing and encryption of the biometric takes places within the Trusted Execution Environment. (TEE as defined in the L1 compliance document)

- It is certified that the TEE has a secure boot process

- It is certified that the TEE supports secure storage of encryption keys in isolated hardware and the same is not exportable by any means outside of the TEE.

- It is certified that the TEE supports asymmetric key signing and encryption (RSA 2048)

- It is certified that the TEE supports for symmetric key encryption (AES 256 GCM)

- It is certified that the TEE supports SHA-256 hashing

- It is certified that the processing, quality checks, preview (if available) are performed in the TEE

- It is certified that the environment has the capability to securely upgrade the software in the TEE
It is certified that there is no external calls/commands/any other mechanism (direct/indirect) to inject a biometric and get the a singed biometric as response.

**Functional Tests**

Functional tests for the essential functions for authentication using registered device specification. Vendor will provide sample client based on UIDAI guidelines for these functional tests.

1. **Device registration/de-registration**
   a. Registration of new device through init function on startup
      ■ Logs of management servers
   b. Successful authentication
   c. De-registration of device through **backend (portal)**
   d. Auth failure due to unregistered device
      ■ This error may be shown error auth code
   e. Re-Register a device through init function on re-start
   f. Auth success on registered device

2. **Device Key rotation**
   a. Configure management server for very short validity of device certificate
   b. Auth failure due to expired device certificate
   c. Rotate certificate through init
   d. Auth success after rotation; verify that new certificate was sent

3. **Upgrading the RD Service**
   a. Auth success
   b. Revoke version of RD service through backend (portal)
   c. Auth failure due to wrong version of RD service
   d. Upgrade the software version of RD service through init
      ■ Init will obtain correct version through service registry xml
   e. Auth success after RD service upgrade

4. **Update device provider certificate**
   a. Auth success
   b. Revoke device provider certificate through backend (portal)
   c. Auth failure due to revoke device provider certificate
   d. Upload new device provider certificate through backend (portal)
   e. Re-sign device key with new device provider key through init
   f. Auth success

5. **Upgrading UIDAI Public Key**
   a. Update incorrect UIDAI public key in RD service
   b. Auth Failure
c. Update correct UIDAI public key through init
d. Auth success

6. Client Functionality
   a. Device Discovery
      i. Single RD Service
      ii. Multiple RD Services
   b. Capture call should provide the device status as per the devices state
      iii. READY/NOT READY/BUSY as per the registered device spec
   c. Preview Validation
      iv. Sub-sampling, distortion
   d. RD service functionality
      v. Optional input parameters, positive and negative test cases

7. Compliance Check
   a. Population: 100 residents who are normally successful with Aadhaar authentication using the relevant modality
      i. Success Rate
         ● UID level success: 98%

8. Poor Quality Biometric Capture Check:
   a. Population: Upto 5 residents typically requiring more than one attempt to do succeed using the relevant modality
      i. Success Criteria
         ● UID level success: 60% success within 5 attempts.

Security Testing:

For the purposes of provisional certification, the following security tests will be performed

Scripted Security Tests:

1. Perform XML injection attacks on the RD services.
   
   Description:
   RD service accepts XML as a valid input and produces XML as an output. The objective in this test case is to inject malicious XML and see the response of the RD Service. We will concentrate on only the listed services as per the UIDAI Spec.

   Steps:
   1. Inject invalid XML.
      a. Invalid XML’s could range from failed XML syntax to valid XML with CDATA and other type of characters. This would evolve, but the OWASP XML injection technique is a good start. https://www.owasp.org/index.php/Testing_for_XML_Injection_(OTG-INPVAL-009)
      2. Inject the invalid XML against all the exposed RD service calls.
Result:

System should respond back the proper XML response as expected for the respective calls (Capture, info) with an error code

Automated Test Case

- The RD service will injected with various XML cheat codes for response.
- The RD service should consistently respond back with correct error codes or should never respond back based on the messages that are sent.
- All the cheat code XML’s will be available in a config folder and more cheat codes can be added to the same.

1. Insert a internet proxy and try inserting keys in the response. Once completed validate if a capture succeeds. Capture call should end with failure

   **Description:**
   This test case is used to ensure that key rotation and other management calls can not be just replayed

   **Steps:**
   1. Use a internet proxy and capture the responses for various interactions that happens between the RD service and the management server.
   2. Try replaying the same response for a different device.
   3. If a value available in the request and response then replace the values appropriately and then replay the response.

   **Results:**
   - The Device/RD service should reject the response and continue to work with this previous known configuration or should attempt more tries.
   - The device/RD service can also move a error state until a proper response is obtained

2. Insert a internet proxy and replace the response from server with a response used for another device. Attempt a capture call and the result should be a failure

3. Remove signature and try upgradation of unsigned files.

4. Make change any of the files to break signature and try upgradation of unsigned files.

**Management Server Certifications:**

5. Audit the HSM and ensure the device provider private keys are generated and stored in the FIPS Level certified HSM and the keys are not extractable.

   **Description:**
   This test case is an audit on the server infrastructure where the private keys are stored.

   **Steps:**
   1. Check the current FIPS level
   2. Check the attributes of the device provider private keys.
Results:
1. The FIPS level should be at a minimum of 140-2 Level 2
2. HSM should have the ability to work in FIPS 140-2 Level 3 to ensure physical protection of keys.
3. The attributes of the device provider private keys should be marked as non-exportable.

6. Perform VA and PT exercise on the server infrastructure

Description:
The test case is just a high level statement and the objective is to ensure the infrastructure is hardened

Steps:
1. Ensure Unwanted services are not running.
2. Only port 80 and 443 is opened for public access
3. Backbone Management ports (SSH or any other) are restricted based on IP or private key.
4. All communication should happen only on SSL.
5. Vulnerability Scan
6. Penetration testing on the management server should be performed.

Results:
The server should be hardened and no open High and Medium Vulnerabilities exist.

Additional Declarations for provisional certification

The vendor must declare that they completed the following tests in their facility and submit test reports. These tests will be performed by STQC/UIDAI during the final certification process.

7. Copy the keystore files to one more device and try using both the devices (L0 only)

8. Try interchanging keystores call capture, The RD service should fail (L0 only)

9. Extract Keystore Files, Perform rainbow table attacks to guess passwords, If the keystore is a file then validate the file permissions and ensure only RD service can access it. (L0 only)

Description:
Keystore files or any other storage location where the keystore is kept should be tested for brute force and rainbow table attacks to validate password strength and ensure proper storage of passwords.

Standard file based keystore:
- Copy the keystore file.

Attempt to break the files using rainbow table based password guess and also use all the list most commonly used password list.

Result:
The password should not guessable and should be dynamic for every device.

Standard hidden file based keystore (windows):
- Attempt to digitally sign using the key.
10. Keystore Validation

**Description:**
Extract Keystore files from device one and place it in device two. See if the device runs and are able to get a capture through RD service.

**File based keystore Steps:**
- If the keystore is a file, then copy the file from the first device (let's call it as Device A) to Device B.
- Run capture command against the RD service of Device B.

**Result:**
The capture should fail with an internal error as it should not have the ability to open the key store.

**Mobile system based keystore steps: (Android, IOS)**
- Ensure the keystore keys are marked to be accessed only by the RD service and not by any other services running on the mobile
- The keys should never be store in the keychain.

**Result:**
The keys are never extractable and that proves that this test as a success

**Windows based keystore steps:**
- Device private keys should not be part of the roaming profile
- Folder location of the keys file has to have permissions only for RD service user account.
- All possible backup access to the keys has to be restricted.
- Copy the files from device A to device B, Ensure the locations are same.
- Once done try the capture service on device B.

**Result:**
The capture should fail with an internal error as its should not have the ability to open the key store.

11. Key Rotation

**Description:**
Continue Test Case 11 and force a key rotation, validate if the RD service capture call provides a pid block

**Steps:**
- Continue the test case 11
- Force a key rotation on the device
- Now call the RD service capture api.

**Result:**
Validate if the RD service return a valid PID.

12. Record & Investigate data
Description:
Record the communication between the RD service and the Physical device.

Steps:
- Capture traffic from the time of installation of driver & RD service till key rotation.
- Keep this information as record.
- Start fuzzing the communication with a mix of valid and invalid data for a predefined duration.
- Record all the data for future reference.

Result:
The result of the exercise is carefully evaluated to determine if there is any leakage of information that could be used by an attacker.

13. Bluetooth wrangling
Description:
In bluetooth devices browse the profiles get information of the device and details. Perform bluesnarfing, crawler and explore bluebug to validate if one of these give more insights

Channel discovery/Exploitation Steps:
- The bluetooth devices communicate over a predefined channel.
- Active scanning for available channels should be performed.
- User bluesnarfing, crawlers and bluebug tools to test the bluetooth on known issues and hidden exposures.

Results:
This exercise will validate for any hidden exposed channels and also will validate if there is any known bluetooth related vulnerabilities that are open.

14. Force Mount USB
Description:
In USB based devices try to force mount the USB drive following the USB mass storage device protocols, it should be impossible to mount.

Steps:
- When a USB is plugged in the operating system a certain message exchanges takes place to determine if the device is mountable.
- In windows most of the work is performed by the usbd.sys file.
- Capture the entire communication and see if we can force the usb mount even when the discover of USB mass storage fails.

Results:
This exercise will ensure that there is no easy access available for the USB based device.

15. Memory Dump the RD Service.
Description:
Force memory dump before and after capture as the RD service and try to find if there is a any secret hardcoded information.

Steps:
1. The latest version operating systems comes with ability to force a memory dump.
2. Use those abilities to force the memory dump.
3. Take few dumps and analyse using the dump analysis tools specific for each operating system.

Result:
System has no hard coded values that a malware could steal

16. Certificate Revocation

Description:
Revoke certificates and see if the RD service is able to validate the UIDAI certificate or device provider certificate revocation. The RD service should fail or attempt to fetch new key from the UIDAI or device provider

Steps:
1. Locally revoke the certificate.
2. Attempt to capture

Results:
Capture should fail and the RD service should attempt to fetch the new certificate from UIDAI servers.

17. Screen record (This is a low profile test and applicable only if the device uses preview display)

Description:
Screen record the fingerprint/iris and see if you can pass it to the extractors.

Steps:
1. Screen capture the image
2. Pass it to the extractor
3. Validate the quality of the extraction.

Results:
The quality should be bad.

18. Integrity Check

Description:
Remove signatures from few of the device driver files. The RD service capture call should fail with error.

Steps:
1. Remove signatures from the dll’s using delcert commands
2. Attempt the capture RD service call

Result
The call should fail as the RD service self validates all its associated set of executables for integrity.

19. Attempt to decompile in case of managed programming languages and validate for store secret

Steps
It’s a simple test case to decompile and validate.

20. Audit if the device has any removable storage or any service mode for replacement

Steps
It’s an audit and self certified.
   **Description:**
   Validate the Product Security Response process, patch management, upgradation
   **Steps:**
   This is a process document to ensure that the device provider has an active way to manage vulnerabilities and fix the same and release it.

22. Code Signing Process
   **Description**
   Signature, malware scanning before signature and other process for safe and secure development release should be followed and evidence for the same to be submitted.

23. Fake UIDAI public key
   **Description:**
   Insert a fake UIDAI public key and validate if the RD service is capable of identifying the wrong cert.
   **Steps:**
   1. Force the device to fetch the fake UIDAI key.
   2. The UIDAI key validation is performed by looking for the CN names and validating CCA certificates.
   3. Perform the capture call through RD service.
   **Result:**
   The RD Service capture call should fail.

24. DNS spoofing
   **Description:**
   Fool the domain name using hosts file where the RD service runs and validate if the RD service is capable of detecting the issue.
   **Steps:**
   1. Spoof the domain name of management server and UIDAI server (The url where the public key is hosted) using the host file for the RD service.
   2. Perform the capture call
   **Result:**
   The RD service should fail because of non https availability.

25. Validate the housing and ensure no external interfaces are provided to connect and input biometric data. Also validate all external connectors for input and output, All USB Channels to be tested as per the usb test cases, All ethernet or wifi channels should undergo Vulnerability assessment and no information should be revealed during a VA. In case of bluetooth we should follow the bluetooth test case as listed above

26. Look for code coverage report and validate if there are public methods exposed.
27. Reverse Lookup
   **Description:**
   Language based lookup for public methods or use the Solution architecture sequence diagram and validate the methods to ensure the methods does not accept external biometric and sign or provide a way to expose private key.

   **Steps:**
   1. Based on the programming language use tools to enumerate the functions.
   2. Validate no methods accepts biometric for signature.

   **Results**
   Validate all the public method and ensure none of it accepts biometric data.

28. Fake Registration
   **Description:**
   Call registration service with random serial numbers and well formatted serial numbers matching the device providers serial number generation.

   **Steps:**
   1. Understand the format.
   2. Enumerate some possible serial numbers
   3. Attempt registration.

   **Results:**
   Registration should fail.

29. In platforms where hooks or interceptors can be used the device should follow strong signing and should also finalize the methods so no extension or interception is used. This can be obtained as self-declaration
Annexure – IV

Level 1 Compliance for Registered Devices

Principles:
Design Mandate
The design key mandate of the UIDAI registered device specification is reproduced below:
“UIDAI does not mandate any specific hardware design and device providers are expected to innovate appropriate form factors for market use. Key design mandate is that registered devices MUST securely sign the biometric data, form the encrypted PID block within the RD Service and give it back to application for use within Aadhaar authentication.
Registered devices MUST ensure the following:
1. There should be no mechanism for any external program to provide stored biometrics and get it signed and encrypted.
2. There should be no mechanism for external program/probe to obtain device private key used for signing the biometrics.”

Level 1 Compliance:
The requirements for level 1 compliance to the registered device specification is reproduced below:
“Device security implementation has level 1 compliance if the signing and encryption of biometric is implemented within the Trusted Execution Environment (TEE) where host OS processes or host OS users do not have any mechanism to obtain the private key or inject biometrics. In this case, management of private keys need to be fully within the TEE”

TEE Definition:
For the purposes of the registered device specification the Trusted Execution Environment (TEE) is implied in the generic sense (and not restricted to Global Platform TEE). The capabilities of the TEE
1. Support for Secure boot
2. Secure storage for keys (separate isolated hardware)
3. Support for PKI encryption and signing using RSA 2048
4. Support for symmetric encryption using AES 256 GCM
5. Support for Hashing using SHA-256
6. Support at the hardware level to isolate the key operations and biometric signing

Only trusted software components from the device provider can be deployed on the TEE. It is expected that PKI (or equivalent) infrastructure will be used to deploy the trusted software.
Suggested certifications for the Trusted Execution Environment include:
1. Common Criteria certification of Global Platform TEE PP
2. Common Criteria certification of Global Platform TPM 2.0 PP
3. Common criteria certification of SE PP
4. FIPS 140-2 certification of Global Platform TEE, Global Platform TPM 2.0, SE
5. EAL 3 or more is a good sign so if anyone has EAL 3 or more we can simply take their certificate and accept.
6. https://en.wikipedia.org/wiki/Trusted_execution_environment#Implementations - Also compliance to the open implementations

Alternatively test reports from the semiconductor vendor showing compliance to the capabilities of TEE may be furnished.
Types of Attacks:
The next most important factor in the design is the mechanisms that are used to perform the attacks. Different
mechanisms of performing attacks are known as attack vectors, and these break down into three classes defined in this document—hack attacks, shack attacks and lab attacks.

**Hack Attack:** A hack attack is one where the hacker is only capable of executing a software attack. Examples of hack attacks include viruses and malware which are downloaded to the device via a physical or a wireless connection.

**Shack Attack:** A shack attack is a low-budget hardware attack, using equipment that could be bought on the high street from a store such as Radio Shack. In these scenarios the attackers have physical access to the device, but not enough equipment or expertise to attack within the integrated circuit packages.

**Lab Attack:** The lab attack vector is the most comprehensive and invasive. If the attacker has access to laboratory equipment, such as electron microscopes, they can perform unlimited reverse engineering of the device. It must be assumed that the attacker can reverse engineer transistor-level detail for any sensitive part of the design - including logic and memories.

In most cases, considering the rule of thumb that states every device can be broken, a device should not try and defend against lab attack directly, but should take measures which limit the damage when a device is broken and therefore make the lab attack uneconomical.

Use of per-device unique secrets is one example where reverse engineering a single device provides the attacker with no useful information; they have the secret for the device that they already own, but not any of the other devices in that class. In the case of Registered Devices, the compromise of one device should not result in a methodology to compromise of other devices.

In addition, the damage is further limited due to the Aadhaar mandate of using multi-factor authentication for high value or high security transactions.

**Intent**
The intent of the registered device specification is to protect against scalable hack and shack attacks and limit damage due to lab attacks.

**Hardware Configuration Review**
This section applies the above principles on various hardware configurations to identify whether they may qualify for Level 1 certification. Every device submitted for certification should first be attempted to classify in one of these categories. If it does not fall into any one of these categories then it is needs to be analyzed from first principles.

1. **Sensor and TEE in a single Integrated Circuit (IC)**

   Sensor and TEE in the same Integrated Circuit (IC). Optionally the IC could have tamper responsive properties, i.e. any attempt to compromise the IC causes the private keys to be wiped out from TEE. The configuration qualifies as Level 1 as it precludes everything except the most sophisticated lab attacks.
2. **Sensor and TEE on Different IC Chips in Same Housing**

Sensor and encryption logic on a single chip (IC1), while the TEE is on a different Chip (IC2). Shared secret to allow encrypted communication between IC1 and IC2. Optionally, secrets in IC1 and IC2 can be protected through tamper responsiveness. This configuration qualifies as level 1 as it precludes everything except the most sophisticated lab attacks.

3. **Sensor and TEE in Same Housing**

In this configuration, Sensor and TEE are present in the same housing, but on different chips, Sensor (IC1) and TEE(IC2). There exists permanent connectivity between IC1 and IC2 which protected within the housing.

While it may be possible with significant effort from a skilled person would be replace the sensor with a malicious component (Shack attack) for single device, this is not scalable. In addition, the fact that all devices are registered with UIDAI by the device providers makes this attack unfeasible. This configuration may be qualified as level 1.

4. **Sensor and TEE as separate packages components:**
In this configuration, Sensor and TEE are packaged separately and there does not exist permanent physical connectivity (connectivity is through USB/Bluetooth etc.) between the sensor and TEE. It may be possible in this cases to replace the sensor with a malicious component using a Shack attack in a scalable manner. **Hence, this configuration does not qualify for level 1 certification.**
Logistics for a Device Provider - Provisional Certification Scheme

Please read Provisional Certification Checklist Document before going through this document. This document focuses on the logistics of obtaining provisional certification.

1. Device Provider should have completed functional testing in the PoC environment extended by UIDAI.
   a. The URLs, Keys and other parameters to be used in the testing (such as rdsId, rdsVer, dpId, mi etc) would be provided by UIDAI to the provider.
   b. Testing can be done over the internet. The provider need not come to UIDAI or get into any formal agreements while testing the Services against the PoC environment.
   c. The provider can use a self-signed key pair in PoC environment. The objective is only to test the functional readiness of Registered Devices Service against Authentication 2.0, Register and De-Register APIs.
   d. Provider will proceed to the pre-production environment only after testing successfully in the PoC environment.
   e. PoC environment will later get merged with Staging environment and sufficient sample codes and test clients will be made available by UIDAI.

2. Provider should take approvals from STQC/UIDAI to participate in the provisional certification process. During this time provider should submit necessary evidence to UIDAI HQ that the functional testing has been completed in PoC environment. The entities will be entertained in the certification scheme only after the clearance from UIDAI. Following details are to be submitted.
   a. Submit a copy of STQC certification of the sensor if available. Provider should confirm in writing or provide an undertaking that the sensor has either undergone STQC accuracy certification successfully or is in the process of certification. **In case the sensor is in the process of certification, the field deployment will happen ONLY post the accuracy certification from STQC**
   b. Provide documentations and declarations in the provisional certification checklist get validation from STQC. This includes solution architecture with traceability matrix, declarations etc.
   c. Provide one or more installable for the RD service, supported models (this should include the model being submitted), OS Name, OS Versions supported for each installables being submitted. UIDAI will assign rdsId and rdsVer accordingly.
   d. Give an undertaking that the provider has procured a Class2/Class3 digital signature or a Class 3 Document signer certificate for the device public key signing purposes for each of its models. The undertaking also should mention that the key is safeguarded in an HSM.

3. Once cleared by UIDAI/STQC, the provider & device details will be created in Registered Devices Ecosystem and a dpId, mi will be assigned accordingly.
4. The provisional certification functional test will be carried out in UIDAI Pre-Production environment.
   a. The provider has to reach UIDAI Technology Centre, Bangalore for demonstrating the functional readiness in Pre-production, after taking a prior appointment.
   b. URLs, licence keys and other facilities to connect to the environment will be provided by UIDAI.

5. The Service Registry will be updated accordingly and the RD services in onboarding phase will be listed in the beta registry.

6. During the testing (onboarding phase), it is not mandatory to use an HSM, instead the keys can be stored in a USB dongle as well - abiding to the CCA mandates for certificates. For production migration, the same keys should be exported to an HSM or a fresh key to be procured in HSM.

7. Provider should demonstrate the functional capabilities of the RD service, Management client and server through a set of semi automated, functional and security tests.

8. Once the functional testing and security tests are completed, and the reports generated are duly validated by STQC, the rdsId/rdsVer will be migrated to production and the production registry XML will be updated accordingly (only if the sensor has already completed STQC accuracy/environmental certification).
Annexure – VI

Answers to Open Queries - RD Discussion Group
Volume 2 (29th March 2017)

1. Integrated devices/PoS devices should be given clear guidelines on the certification.
   
   Please see provisional certification checklist

2. For PoS if the OEM for the Biometric Sensor/Extractor is not going for certification what to do?
   
   Please see provisional certification checklist

3. Guidelines for platform independent devices should be provided (They don’t know which OS will get inside the PoS)

   If the extraction/quality signing, encryption is done inside the “platform independent“ device only one RD service is required to be certified. Otherwise, separate RD services are required for each platform. Provisional certification will be done at UID Tech Centre (under STQC supervision) and automated reports generated for final sign off at STQC

4. Definition of TEE for Level 1 compliance?

   Please see Level 1 compliance document

5. As per the IT Act an HSM used for the purpose of signing needs to be under exclusive control of the entity / organisation doing the signing. Does this mean that cloud / co-located or outsourced implementations do not qualify and only an on-premise deployment is legally valid?

   Management server may be on an India based cloud setup, or co-located within a data center within India. Device provider can use a third party technology service provider (TSP) to run and manage the setup with a contractual arrangement. HSM, whether it is cloud based or dedicated or shared, must be part of the production network where management server is running and must be protected through network and strong access control mechanisms. Appropriate audit and monitoring must be established for entire management server production environment including HSM.

6. Clarity on STQC Certification (Provisional/Actual)
   a. What test will be performed

      See provisional certification checklist

   b. Which documents to be submitted

      See provisional certification checklist
c. Timelines:

See provisional certification checklist

d. How many devices to be submitted

See provisional certification checklist

e. What is getting certified? (Device/RD service/Management server)

RD Service (Extract/Process/Preview, Sign and Encrypt)

f. Details on when should a recertification or Delta Certification should be done (Both FRR and RD)

Mini accuracy list will be done with provisional certification

g. Will there be different certification for difference RD service versions?

Yes, change in version will cause re-certification

h. Will provisional certification issuance continue till 31st December?

Currently available till June 1st, 2017

i. Costs involved in certification

STQC to publish

j. List of test cases to be shared with vendor

Test Rig will be shared with the vendor

k. What Debug options to give to STQC when the device is submitted

With regards to L1 devices this needs to be proposed by the device provider

l. How the tamper resistiveness will be tested for L1 Certification

For L1 devices with tamper resistance, test cases have to be agreed upon with device vendor

m. Only FRR certified devices can participate provisional certification? Is there any sequence for FRR testing vs RD certification.

Priority will be given for sensors already in the field. However, any device vendors who have applied for STQC certification may participate in the RD service provisional certification
7. As per the document (aadhaar_registered_devices_2_0_1) Pid encryption and Session key encryption shall be done inside the device hardware. So we have following understanding regarding the storage of Uidai public key certificates. The Management server will be pushing the updated versions of the Certificates (“P”, “PP”, “S”) to Management Client. Management client will be responsible for storing these certificates inside the host device. Please confirm this.

Yes, confirmed. RD service should store, upgrade, and use UIDAI public keys used for PID encryption.

8. Management Server: Please confirm if this can be hosted on a cloud outside India. The specification does not mandate where this server has to be hosted and since this is a critical component in ensuring that key rotation takes place successfully and does lead to down_time, OEMs / Device providers would like to host it as per their convenience and confidentiality.

Management server must be hosted in India

9. Certification Scheme readiness: Please provide a timeline by when the certification scheme will be ready and vendors can approach STQC for applications.

Final scheme incorporating feedback from vendors expected to be released by end of March. Vendors can approach STQC for certification immediately

10. Also can we list down additional testing facilities to avoid crowding and ensure that vendors can get certified simultaneously?

Provisional certification will take place at the UIDAI Tech Centre in April and May. Every effort will be made to automate and streamline provisional certification.

11. Integrated FP Devices: Please clarify that this includes only mobile phones / tablets with integrated fingerprint modules and not POS devices with integrated fingerprint modules. POS with integrated FPS are already deployed in the field and will also have to get certified under the current testing scheme.

See certification guidelines

12. External test laboratory/ client’s test facility may be used to conduct the testing (where test facilities are not available with STQC): Please clarify how will this be handled in case clients test laboratory is set up outside India

Test reports from the test facility would submitted as part of the final certification.

13. Level 1: Current STQC certified public devices have been tested with a particular sensor + extractor combination. There is a specific version of the extractor which was used to certify these devices in a PC based environment. When moving to Level 1, the version of the extractor will change as the version which was used for PC based will not give the same performance in an embedded scenario.

Refer to provisional certification checklist.
14. Please clarify that UIDAI will allow already certified device providers to make this change in version number as long as the sensor + extractor combination is not broken. If not, will we have to go again through FRR in such scenario?

Refer to certification guidelines.

15. The spec mentions that the management client needs to be authenticated during registration and certificate signing. Some possible methods are username / password or some form of OTP. In case the password or the OTP device is compromised on the customer side and a non-genuine client is registered would this be a liability for the device provider? If so, how can this be avoided?

Need to establish a secure channel between management client and server. Initial registration may require additional data to ensure only valid devices of the provider are connected to management server. Out of band channel may be used for first establishment of trust.

16. What are the events or origins of De-Registration operation?

If the Management Server/UIDAI admin decides that a device has been taken out of service/compromised in may be deregistered.

17. Is TEE "Trusted Execution Environment" is just a generic term used by UIDAI to refer to Housing both Biometric Sensor(s) and Computing Chip with Crypto Algorithms and that the housing is Tamper Proof and Tamper Resistant?

Are you referring to TEE as defined in WikiPedia with Standardization Specifications by GlobalPlatform? https://en.wikipedia.org/wiki/Trusted_execution_environment

   a. Is it required to provide internationally relevant certifications?

   b. How to define the relevant TEE certificate?

   c. Normally, it is provided to mobile vendors. Is it accepted if we use the components which has passed the TEE? or the device need to pass the TEE as a whole set?

See L1 compliance document for more details.

18. Is the current Level 1 Certification only consider Physical Attacks on Device? Or even advance attacks like Thermal, Differential Power Analysis, Electron Microscope are included?

See L1 compliance document for more details

19. Please clarify on SubSampling of Biometric Image for Preview Purpose

   d. How do we validate the preview is safe?

   e. What Resolution of the Image should be safe that the Image is not usable?
f. Can Animation or Messages alone to guide User is acceptable?

*Just using animation and visual feedback is fine. A user or a screen capture software should not be able to image capture the preview and successfully perform biometric matching.*

20. There will not be a specific software upgrade mechanism for Management client, but the issues with Management client will be fixed when we perform a SW O.S upgrade of the complete device.

   a. Hope this approach is fine as long as we have a mechanism to upgrade the Management client. *Management server/client should detect the need for upgrade if any and trigger. Actual upgrade can be part of common OS upgrade and can be from standard upgrade mechanisms such as playstore etc.*

21. Management server will not push the software upgrades, but we have a Google certified method using which standard Android O.S upgrades will pushed to all client devices by Samsung maintained server for O.S upgrade.

   b. Hope this approach is fine as long as we have a mechanism to push SW upgrades to the Management client. *Management server/client should detect the need for upgrade if any and trigger. Actual upgrade can be part of common OS upgrade and can be from standard upgrade mechanisms such as playstore etc.*

22. In aadhaar_registered_devices_2_0_1.pdf It is mentioned two actions INFO and CAPTURE should be supported. It means we have to provide Activities to handle this actions. As we understand when CAPTURE action is called we should show a preview Activity for iris and PID_DATA should be returned in result (onActivityResult()).

   a. Some B2B applications want their own customized preview instead of an activity. They would expect a consistent UX design language through their entire app. How should this be handled? Can separate callback APIs be provided for custom preview?
   
   b. Incase of INFO action what is to be shown apart from giving the device info result in onActivityResult?

   *No. RD service should NEVER return biometrics in any form. Preview must be done within the RD service and no APIs must be available to apps for obtaining biometrics even for preview. For INFO, no UI is mandated.*

23. "AUAs can buffer authentication requests and send it to Aadhaar authentication server to support occasional lack of network connectivity on the field. Maximum time up to which requests can be queued (buffered) will be defined by UIDAI policy. Currently, this will be configured to 24 hours and may be changed as per policy. All requests with “ts” value older than this limit will be rejected." - It means the encrypted pid having signed biometric can be stored and used for authentication later any time between next 24 hours. Doesn't this mean that the pid block is susceptible for usage without the users consent at a later point of time?. So we think this time should be reduced to a short time interval.

   *Time allowed for buffered authentication will be reviewed by UIDAI from time to time. AUAs must comply with the policy. Authentication requests older than policy window will be rejected.*
24. The below XML is given in the document for Windows/Linux Device discovery

```xml
<RDService status="READY|USED|NOTREADY|..." info="provider info for display purposes">

<Interface id="CAPTURE" path="/rd/capture" />

<Interface id="DEVICEINFO" path="/rd/info" />

</RDService>
```

c. Is that we need to use the same XML for android RD_SERVICE_INFO parameter while calling INFO intent?
d. IF so what are the informations we have to specify in Interface id and path?

Yes. You can pass "fully qualified activity class name" as part of path.

25. We have the queries in fingerprint preview.

In STQC test cases Solution Architecture (page number 8 and point D) the STQC have specified the below point. Describe the sequence diagram for “capture” function implementation

- Quality check, Preview, Capture Sequence etc
- Is there any specification to show fingerprint preview for L0 and L1 devices?

If this feature is implemented, the image must be distorted and undersample to extent that anyone capturing the preview image cannot successfully use the image for fingerprint matching.

26. For L1 device, how to preview the image for both fingerprint/iris devices?

Preview can be on a secure display on a L1 device.

27. My question is related to capture_and_sign service on Android. As per my understanding of L0 devices, Android keystore is possibly an acceptable method to generate and store device key pair. I am aware that Android keystore allows developers to specify access control, key usage policies and lifetime during import/generation of keys. Who would be held liable for key compromise in case if Android device gets rooted and access control rules are modified in a way that a malware can use device private key to sign desired biometrics?

In the case of L0 device, liability for compromise due to rooting (or other compromise) of the host belongs to AUA and not the device provider.

28. As part of the specification there is a mention about Software Upgrades:

a. "Management client should check for software upgrades and initiate upgrades"
b. "Management server should authenticate management clients and allow registration, key rotation, triggering upgrades, and other necessary management services. See previous section for details."

We (Vendor) have well established method using which we perform Android O.S upgrades (SW Upgrades) and other security patch upgrades for all our devices and similarly the same method will be followed for Integrated Iris devices. In case of Iris Tab, management client will be a system service (enhanced security) which will be bundled along with the system Framework of the Device Binary and the same will be upgraded when the O.S upgrade happens.

Please clarify the following: [Especially for Integrated Mobile/Tab form factor devices]

- There will not be a specific software upgrade mechanism for Management client, but the issues with Management client will be fixed when we perform a SW O.S upgrade of the complete device. Hope this approach is fine as long as we have a mechanism to upgrade the Management client.

  *This approach is OK*

- Management server will not push the software upgrades, but we have a Google certified method using which standard Android O.S upgrades will pushed to all client devices by Samsung maintained server for O.S upgrade. Hope this approach is fine as long as we have a mechanism to push SW upgrades to the Management client.

  *The approach is fine. However, L1 compliant devices must have a method to secure software update to trusted execution environment.*

29. Management service should trigger key rotation under 2 scenarios:

- based on the trigger from management server during "init" (ideally done at least once a day);
- based on the manual trigger from management client UI (this is needed only in special conditions where manual key reset needs to be triggered). This trigger should call same "init" to re-initialize.

So the point basically means that Management Client will be a (Service+UI) running on the client end, which will automatically call init? Or management client will be a UI based client which will be invoked manually for Init operation.

*Init should be automatic by default, UI is just an optional back up*

30. Whether Management Client is an UI based application which will be invoked manually or it is a combination of Service, UI based interface to manage the device "Init" (Register for first time and other operations) automatically as soon as device is detected. From the point (5a in registered device document) mentioned in previous mail indicates that it will a service managing Key Rotation on a trigger from management server during init, source of invocation of Init operation is not clear.

*UI is optional for the management client. Init functionality that is triggered when a device is detected is mandatory. Init should decide whether, registration, key rotation, RD service update, UIDAI public key update are required.*

31. Is there any recommendation for the **txn** attribute value in Register/DeRegister APIs? Or we can follow the same format being used for Authentication request.
**Same format as authentication request**

32. We are requesting STQC certification on cloud hsm or evaluation box. Can you please have it confirmed as acceptable?

**Please see Logistics for provisional certification**

33. Debug Board for L1 Compliance Description: Device Vendor will provide a debug board with appropriate probe points to verify their device meets the requirements for L1 compliance. Steps: Details of the board, probe points and methodology will be outlined by the vendor in their submission. Result: Success criteria consistent with L1 compliance will be outlined by the vendor.

*See L1 compliance document for more details.*

34. STQC Guidelines: Page 4 (Point 5) – Inputs Required by STQC for provisional Certificate (L0 Device)
   a. What are the criteria for provisional certification for L0 Device?
   b. STQC FRR Certificate and ETDC Mohali Testing Report are asked. It means that provisional is only for already certified devices. Please clarify this.

*Device provider can apply for provisional certification for any sensor certified by STQC*

35. STQC Guidelines: Page 7 (Checklist) Phase I: A provisional certificate will be issued in the first phase having a validity till Dec 31st 2017. It is expected that provisional certificates will be issued starting Mar 15th 2017.
   a. When the window of provisional certificate issuance will be over?

*Provisional certificate testing window will continue till 1st June 2017*

36. STQC Guidelines: Page 4 (Point 5) – Inputs Required by STQC for provisional Certificate (L1 Device)
   a. What are the criteria for provisional certification for L1 Device?
   b. Whether FRR Certificate or ETDC Mohali Test Report is needed? Please confirm.

*Please refer the provisional certificate checklist*

37. STQC Guidelines: External test laboratory/ client’s test facility may be used to conduct the testing (where test facilities are not available with STQC).
   CMT>> What type of tests would be carried outside STQC and in which scenario this will be applicable. Is this relevant for Level0. Please elaborate.

*Refer to certification guidelines.*

38. STQC Guidelines: Test Tool / Software would be provided by UIDAI.
   CMT>> When will this tool be available? Will this tool be available in C code? It is needed to have a tool which can run on any device and which can be compiled in any platform.

*Tool will be provided shortly.*
39. STQC Guidelines: Vendor to provide test points / probes tools & techniques to demonstrate of compliance along with an undertaking for meeting the requirement. Is this applicable for Level 0? If yes then what type of test points and probes tools expected? Please elaborate.

   This is relevant only for Level 1 certification

40. STQC Guidelines: Is the Preview of the image a requirement? We would rather recommend to just give visual feedbacks. Users are no biometric experts and it should be the system to determine quality for the submission and not the operator.

   Preview is not a requirement; in fact, visual feedback such as guides etc. are preferred.

41. STQC Guidelines: "Functional tests test the essential functions for conducting the authentication using registered device specification. This step is mandatory for even for provisional certification. Vendor will provide sample client based on UIDAI guidelines for these functional tests." - How will errors be introduced? Should we have a set of expired certificates? What about the version of the server? Should we have two servers to hit one being with the wrong version?

   Will be clarified as part of the test rig

42. STQC Guidelines: Are following test cases applicable for L0 device if the key store is implemented in TEE?

   1. Extract Keystore Files, perform rainbow table attacks to guess passwords, If the keystore is a file then validate the file permissions and ensure only RD service can access it.

   Description:

   Keystore files or any other storage location where the keystore is kept should be tested for brute force and rainbow table attacks to validate password strength and ensure proper storage of passwords.

   Standard file based keystore:

   ● Copy the keystore file.

   ● Attempt to break the files using rainbow table based password guess and also use all the list most commonly used password list.

   2. Keystore Validation

   Description:

   Extract Keystore files from device one and place it in device two. See if the device runs and are able to get a capture through RD service.

   File based keystore Steps:

   ● If the keystore is a file, then copy the file from the first device (let's call it as Device A) to Device B.

   ● Run capture command against the RD service of Device B.
10. In L0 copy the keystore files to one more device and try using both the devices
a. The test cases are same as that of keystore validation test case
11. Try interchanging keystores in L0 and call capture, The RD service should fail
a. The test cases are same as that of keystore validation test case

Vendor Comment:

As part of Product Level 0 upgrade we are implementing the key store in Trusted Execution environment (HW based Key store) hence it won’t be possible to Extract and validate the keys. Note: Though as part of Level 0 specification it is not mandated to go with Trusted Execution environment (HW based Key store) for enhanced security we have implemented the key store in TEE.

*If keystore is being implemented in a TEE for an L0 device, then test cases related to L0 keystore testing may be exempted.*

43. STQC Guidelines: Are following test cases applicable for integrated devices?

4. Record & Investigate data

Description:

Record the communication between the RD service and the Physical device.

Steps:

● Capture traffic from the time of installation of driver & Rd service till key rotation.

● Keep this information as record.

● Start fuzzing the communication with a mix of valid and invalid data for a predefined duration.

● Record all the data for future reference.

5. Bluetooth wrangling

Description:

In bluetooth devices browse the profiles get information of the device and details. Perform bluesnarfing, crawler and explore bluebug to validate if one of these give more insights Channel discovery/Exploitation Steps:

● The bluetooth devices communicate over a predefined channel.

● Active scanning for available channels should be performed.
- User bluesnarfing, crawlers and bluebug tools to test the bluetooth on known issues and hidden exposures.

6. Force Mount USB

Description:

In USB based devices try to force mount the USB drive following the USB mass storage device protocols, it should be impossible to mount.

Steps:

- When a USB is plugged in the operating system a certain message exchanges takes place to determine if the device is mountable.
- In windows most of the work is performed by the usbd.sys file.
- Capture the entire communication and see if we can force the usb mount even when the discover of USB mass storage fails.

Vendor Comment:

The above mentioned test cases is not applicable to integrated Mobile/Tab form factor devices.

*For integrated devices (on mobile phone/Tab) the force mount USB and Bluetooth Wrangling test cases are not relevant.*

44. STQC Guidelines: Are following test cases applicable for Android based integrated devices?

17. Integrity Check

Description:

Remove signatures from few of the device driver files. The RD service capture call should fail with error.

Steps:

1. Remove signatures from the dll’s using delcert commands
2. Attempt the capture RD service call

Vendor Comment:

The above mentioned test case is not applicable for Android based integrated devices, because RD service is a system service which is implemented as part of the system Framework.

*These are not required.*
45. STQC Guidelines: Code Signing Process Description
Signature, malware scanning before signature and other process for safe and secure development release should be followed and evidence for the same to be submitted.
Do we need to sign our code or just provide an MD5 hash?

MD5 is for installable file. Signing of code is a separate issue.

46. STQC Guidelines: Page 3 (Last Para) Compliance may be verified based on the test reports &/or certifications obtained by the client.
   a. What are the certifications/Test Reports are allowed from client? This should not be subjective in nature.
   Please see the provisional certification checklist.

47. STQC Guidelines: Please clarify on Memory Dump
   a. Is it should be part of the Production Software?
   b. What is the tool to test Memory Dump?

   In case of L0 it's a dump initiated from the operating system. You can use ProcDump utility of Windows or Linux Memory Extractor for linux and android to achieve the same.

   In case of L1 device it's a dump initiated from the debug board and the tools and process to do could differ.

48. STQC Guidelines: Can we have more details on this “Start fuzzing the communication with a mix of valid and invalid data for a predefined duration. “

   Assuming this is for the STQC, the link has the basics on USB fuzzing http://blog.quarkslab.com/usb-fuzzing-basics-from-fuzzing-to-bug-reporting.html

49. STQC Guidelines: “The result of the exercise is carefully evaluated to determine if there is any leakage of information that could be used by an attacker.” Who will be evaluating the threat model?

   The person who is involved in testing is expected to perform this activity. The expectation from the tester is to look at the communication that comes back from the USB or serial terminal and read through the data to see if any information leakage exist or any clue to backdoors are shown

50. STQC Guidelines: For Testing & Certification, can we use cloud hsm or evaluation boxes supplied by hsm vendors. To procure and put it on commercial setup may not be possible in given timelines.

   Cloud HSM is fine or evaluation hsm is also fine. But the setup has to be in production before the first device registers and the same is validated during full certification.

51. STQC Guidelines: Keystore Validation Description: Extract Keystore files from device one and place it in device two. See if the device runs and are able to get a capture through RD service. File based keystore
Steps: ● If the keystore is a file, then copy the file from the first device (let’s call it as Device A) to Device B. ● Run capture command against the RD service of Device B. Result: The capture should fail with an internal error as its should not have the ability to open the key store. Mobile system based keystore steps: (Android, IOS) ● Ensure the keystore keys are marked to be accessed only by the RD service and not by any other services running on the mobile ● The keys should never be store in the keychain. Result: The keys are never extractable and that proves that this test as a success Windows based keystore steps: ● Device private keys should not be part of the roaming profile ● Folder location of the keys file has to have permissions only for RD service user account. ● All possible backup access to the keys has to be restricted. ● Copy the files from device A to device B, Ensure the locations are same. ● Once done try the capture service on device B. Result: The capture should fail with an internal error as its should not have the ability to open the key store.

“Restricting access to Admin account may not be possible. Restricting access to programs below the file system may not be possible. Please comment”

Yes there could be some loopholes but the expectation is that to ensure the admin logins are not the default and they are disabled and can be used only in special conditions. Enabling hard disk based encryption ensures that the programs below the file system can not access. Let us try the best to protect there is always a way to break but we can not handover the keys without a fight.

52. STQC Guidelines: Record & Investigate data Description: Record the communication between the RD service and the Physical device. Steps: ● Capture traffic from the time of installation of driver & Rd service till key rotation. ● Keep this information as record. ● Start fuzzing the communication with a mix of valid and invalid data for a predefined duration. ● Record all the data for future reference. Result: The result of the exercise is carefully evaluated to determine if there is any leakage of information that could be used by an attacker.

“Is there a test tool for this? Who will provide it? The test is very open ended with no specific success / failure criteria”

Yes its open ended and its part of the information gathering phase of the ethical hackers. This is standard practice in any of the Ethical Hacking procedure.

53. STQC Guidelines: Force Mount USB Description: In USB based devices try to force mount the USB drive following the USB mass storage device protocols, It should be impossible to mount. Steps: ● When a USB is plugged in the operating system a certain message exchanges takes place to determine if the device is mountable. ● In windows most of the work is performed by the usbd.sys file. ● Capture the entire communication and see if we can force the usb mount even when the discover of USB mass storage fails. Results: This exercise will ensure that there is no easy access available for the USB based device

“Is there a test tool for this? who will provide it?”

As of now its expected that the Security Testing vendors should provide it, In linux these are simple ones to
54. STQC Guidelines: Perform XML injection attacks on the RD services. Description: RD service accepts XML as a valid input and produces XML as an output. The objective in this test case is to inject malicious XML and see the response of the RD Service. We will concentrate on only the listed services as per the UIDAI Spec. Steps: 1. Inject invalid XML. a. Invalid XML’s could range from failed XML syntax to valid XML with CDATA and other type of characters. This would evolve, but the OWASP XML injection technique is a good start. https://www.owasp.org/index.php/Testing_for_XML_Injection_(OTG-INPVAL-009) 2. Inject the invalid XML against all the exposed RD service calls. Result: System should respond back the proper XML response as expected for the respective calls (Capture, info) with an error code “Will using available industry standard XML parsers handle this issue or are further steps to be taken? “

_Industry XML parsers have settings that enables you to handle this better. So understanding you libraries to a good extent will help. Most of these parsers provides options to disable all advanced usages._

55. STQC Guidelines: Memory Dump the RD Service. Description: Force memory dump before and after capture as the RD service and try to find if there is a any secret hardcoded information. Steps: 1. The latest version operating systems comes with ability to force a memory dump. 2. Use those abilities to force the memory dump 3. Take few dumps and analyse using the dump analysis tools specific for each operating system. Result: System has no hard coded values that a malware could steal “The test is very open ended with no specific success / failure criteria. Please comment”

_If you find the key in the memory dump then that's a failure. You can use tools mentioned above for memory dump or use the forensic tools which are equipped to handle this better._

56. STQC Guidelines: Audit the HSM and ensure the device provider private keys are generated and stored in the FIPS Level certified HSM and the keys are not extractable. Description: This test case is an audit on the server infrastructure where the private keys are stored. Steps: 1. Check the current FIPS level 2. Check the attributes of the device provider private keys. Results: 1. The FIPS level should be at a minimum of 140-2 Level 2 2. HSM should have the ability to work in FIPS 140-2 Level 3 to ensure physical protection of kyes. 3. The attributes of the device provider private keys should be marked as non exportable.

“It is not clear whether level 2 is acceptable or if level 3 is mandatory”

_In case of Cloud HSM Level 2 is the max that can be provided. So Level 2 is fine._
57. STQC Guidelines: Insert a internet proxy and try inserting keys in the response. Once completed validate if a capture succeeds. Capture call should end with failure Description: This test case is used to ensure that key rotation and other management calls can not be just replayed Steps: 1. Use a internet proxy and capture the responses for various interactions that happens between the RD service and the management server. 2. Try replaying the same response for a different device. 3. If a value available in the request and response then replace the values appropriately and then replay the response. Results: ● The Device/RD service should reject the response and continue to work with this previous known configuration or should attempt more tries. ● The device/RD service can also move a error state until a proper response is obtained.

“Is this required if the connection is going to be HTTPS?”

Yes HTTPS is one of the most tricky protocol and provides lot false protections so we should never assume that it’s good. We should always assume we have a wifi network from where MITM is possible.

58. STQC Guidelines: Integrity Check Description: Remove signatures from few of the device driver files. The RD service capture call should fail with error. Steps: 1. Remove signatures from the dll’s using delcert commands 2. Attempt the capture RD service call Result The call should fail as the RD service self validates all its associated set of executables for integrity.

“Does this refer to vendor standard SDK / API library signing? Certain OS may not mandate this. Is it required for all OS?”

In all windows, Mac and Mobile (Android, IOS, Windows ) platforms this is mandatory.

59. On what conditions **init** will be triggered?

**init** will be triggered during following conditions.
1. Mandatory init at least once in every 24 hours.
2. When a new device is connected
3. When the RD Service is restarted. (Instead of manually restarting the service and invoking an **init**, a force init option can be provided at the management console of the RD Service – It is important to note that the AUA application SHOULD NOT have access to invoke Init calls)

60. Can RD service access external URLs?

RD Service should not connect to 3rd party servers on the Internet other than those servers managed by the Device provider or the OS provider (in case of playstore update etc.) or of the agency using the device (e.g., AUA managed environments) to avoid any malware attack. RD Registry, UIDAI keys, device keys, etc must be managed through the management server and RD service should not directly contact UIDAI servers

61. What should be the frequency of referring to the Service Registry XML by the management server?

Management server should read and cache the registry XML at least once in 24 hours.
62. What minimum should the management server do when an `init` call is received?

Management server should decide and implement following when an `init` call received.

- Is device registration required?
- Is key rotation required?
- Is RD service update required?
- Is UIDAI public key rotation required?
Application form for Registered Devices Certification
## Application for Testing and Certification of Registered Devices for UID Application

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Name &amp; Address of Supplier (Client / Agent/ Channel Partner /Applicant)</strong>&lt;br&gt;Also mention Tel, Mobile, Fax, email&lt;br&gt;Contact Person if different from above&lt;br&gt;(Also mention Tel, Mobile, Fax, email)</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Name &amp; Address of Registered Device Manufacturing organization</strong>&lt;br&gt; If different from above&lt;br&gt;(Also mention Tel, Fax, email)</td>
</tr>
<tr>
<td>3.</td>
<td><strong>Description of the Registered Device</strong>&lt;br&gt;\ a) Fingerprint Scanner&lt;br&gt;\ b) Iris Scanner</td>
</tr>
<tr>
<td>4.</td>
<td><strong>Nomenclature / Model No.</strong>&lt;br&gt;<strong>Sensor Reference No.</strong>&lt;br&gt;<strong>Extractor Reference No.</strong>&lt;br&gt;<strong>Version &amp; Year of manufacturing/ release</strong>&lt;br&gt;(For integrated device Model No. plus 5 critical components)&lt;br&gt;*Note: fill separate application for each type of device*</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Reference of technical construction file</strong></td>
</tr>
<tr>
<td>6.</td>
<td><strong>Fee details as submitted</strong>&lt;br&gt;(Indicate amount and the DD details/ transaction number in case of ECS payment)</td>
</tr>
<tr>
<td>7.</td>
<td><strong>Application filled in by</strong></td>
</tr>
<tr>
<td>8.</td>
<td><strong>Tested from UIDAI Tech Center</strong>&lt;br&gt;Bangalore in staging environment</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Date</strong></td>
</tr>
</tbody>
</table>
Declaration:

- I will abide by all the Rules and Procedures of the Certification body.
- I agree with the terms and conditions of the certification body.
- I agree with the schedule of Charges of certification body.
- I agree with certification agreement

(Authorised Signatory)

Enclosures to be submitted

a) Testing and Certification fee in Demand Draft / ECS
b) Copy of the certificate issued by STQC (if any)
c) Reference of Test report number from BDTL Mohali
d) Certificate/ Letter of accuracy of FRR
e) Certification Agreement two copies duly signed
f) Three Nos. of Registered Devices along with SDK, API and driver software etc. (VDM).
g) Technical Construction File

The Application along with relevant documentation as above is to be submitted to:

Director STQC, Room NO. 3061,
6 CGO Complex, Lodi Road New Delhi-110003. Tel.No. 24301361,
Email: abanati.stqc@nic.in

h) The Test samples along with a copy of application & documents to be submitted to:

Director, Biometrics Device Test Laboratory, ETDC, NA Block B-108,
Industrial Area VIII Mohali (Panjab) Tel.No. 0172-2237576/2236707
Email rsahi.stqc@nic.in