Guideline to Applicant for Registered Device Service Testing

(STQC/BDCS/P12)

Issue: 01

Biometric Device Certification Scheme (BDCS)
STQC Directorate,
Ministry of Electronics & Information Technology (MeitY)
Government of India

Contents

0.1 Approval and Issue ... 3
0.2 Amendment Record ... 4
1. Background ... 5
2. Reference Documents ... 5
3. Target Audience ... 5
4. Purpose & Objectives of Testing and Certification ... 5
5. Scope of Work ... 6
6. Inputs Required by STQC for Provisional Certificate ... 7
7. Activities to be performed ... 7
8. Deliverables ... 8
9. Test and Certification Schedule ... 8
10. Mode of Payment ... 8
11. Terms and Conditions ... 8
12. Abbreviations ... 8
Annexure – I List of applicable UIDAI specifications / documents ... 10
Annexure – II Checklist for Provisional Certification of Registered Device (RD) Service ... 11
Solution Architecture: ... 11
Declarations (L0 & L1 both): ... 16
Declarations for L1 Devices only: ... 17
Functional Tests ... 18
Security Testing: ... 20
Scripted Security Tests: ... 20
Management Server Certifications: ... 22
Additional Declarations for provisional certification ... 24
Annexure – III Logistics for a Device Provider - Provisional Certification Scheme ... 35

0.1 Approval and Issue

Reviewed by : Management Representative

Approved by : Head, BDCS

Note:

- Management Representative (MR) is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

0.2 Amendment Record

Sl. No.	Date	Issue	Rev.	Reason of Change /Change Details
1.	04-01-2021	1	0	First Issue

1. Background

Biometric Device Certification Scheme (BDCS) is operated by STQC Directorate, Ministry of Electronics and Information Technology (MeitY), Govt. of India. Under supervision of CB, the Testing Laboratories or Biometric Device Test laboratory (henceforth will be referred as BDTL) perform Testing of Biometric Device products against the requirements of UIDAI.

UIDAI Requires that only registered devices should be used by all Authentication Eco partners.

"Registered Devices" refer to devices that are registered with Aadhaar system for encryption key management. Aadhaar authentication server can individually identify and validate these devices and manage encryption keys on each registered device.

- **Device identification** – every physical sensor device having a unique identifier allowing device authentication, traceability, analytics, and fraud management.
- **Eliminating use of stored biometrics** – every biometric record is processed and encrypted within the secure zone eliminating transmission of unencrypted biometrics from sensor to host machine.

2. Reference Documents

STQC/BDCS/D01	:	Rules and Procedures
STQC/BDCS/D08	:	Specifications
STQC/BDCS/F01	:	Application
ISO 27001	:	Information Security Management System

Aadhaar Registered Devices – Technical specification, latest version

L1 traceability matrix document

System security engineering (NIST SP 800-160)

*(Please refer **Master List of Documents** for latest version of the documents)*

3. Target Audience

The Supplier of Biometric Authentication devices, STQC Test Laboratory and the Certification body shall follow this procedure for certification.

4. Purpose &Objectives of Testing and 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 Aadhaar Registered Device Technical Specification achieving L0 or L1 compliance.

b) To verify that the DUT meets all environmental, safety and accuracy requirements as per

required specification.

c) Provide opportunity forVendors 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.

5. Scope of Work

The scope includes testing & certification of the following Biometric Authentication 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 BDTL will now be tested for compliance to the UIDAI registered device specification.
- 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 specifications (latest version)".

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 traceabilitydocumentfromUIDAIrequirementtosolutionarchitecture.Operationaldemo by the vendor.
- Execution of test cases with tools & scripts provided byUIDAI
- Security tests listed as perappendix
- 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.

6. 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 – Biometric device specifications compliance, Authentication API compliance documentation, Register Device specification compliance
- Device Documentation–RD Service Documentation, Management Client Documentation, Management Server documentations
- Authentication client for testing purposeonly.
- FRR Testing Report
- BDTL Test Report
- Test environment for testing of specialized security parameters (if required)
- Internal test reports ofclient
- 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.

7. Activities to be performed

1. Testing Activities:

a. Study & Understanding security of Registered Devices
b. Test Planning & Preparation
c. Test Execution
d. Test Report Preparation

2. Certification Activities:

a. Analysis of test results
b. Verify compliance to evaluation criteria
c. Issue of Certificate (if evaluation criteria is met)

8. Deliverables

The following deliverables will be provided to the client:

- Security Test Report
- Certificate, subject to fulfilment of evaluation criteria

9. Test and Certification Schedule

- It will take about 6-8 weeks to complete the testing and certification after required inputs have been provided by the client to STQC.
- The charges for testing and certification (**Refer STQC/BDCS/D02**) will be as per the schedule of charges and Test report/Certificate will be issued only after receipt of test certification fees.
- The GST shall be extra as applicable.

10. Mode of Payment

Applicable charges are required to be paid in advance through BharatKosh (bharatkosh.gov.in) only in favour of concerned laboratory.

11. Terms and Conditions

- The payments to STQC Directorate (being Government of India organization) are exempted from TDS under section 196 of Income Tax Act.
- The vendor shall arrange for DUT and support environment at STQC test lab where testing will be undertaken.
- The client shall arrange for DUT and support environment at STQC test lab where testing will beundertaken.
- In order to complete the testing, as per schedule, client shall ensure readiness of test related documentation and timely availability of the requiredinformation.
- Test Laboratory shall ensure timely completion of test activities as per plan and submit the deliverables.

12. Abbreviations

BDCS	- Biometric Device Certification Scheme
CB	- Certification Body
CC	- Certification Committee
DUT	-Device under test
STQC	- Standardization Testing Quality and Certification Directorate

UIDAI - Unique Identification Authority of India
RDS - Registered Device Service

Annexure – I List of applicable UIDAI specifications / documents

1. AADHAAR REGISTERED DEVICES TECHNICAL SPECIFICATION - VERSION 2.0 (REVISION1)
   http://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_1.pdf

2. AADHAR AUTHENTICATION API SPECIFICATION –VERSION 2.0 (REVISION 1)
   https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

3. Registered Devices Addendum Document for ErrorCodes
   https://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_1_error_codes.pdf

Annexure – II Checklist forProvisional Certification of Registered Device (RD) Service

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.

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. 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 (Refer STQC/BDCS/F11- Template) 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 is not possible to insert a (stored) biometric in to 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. L1Compliance:

- Show how the biometrics are signed and encrypted within the trusted execution environment. (Firmware or HardwareSolution)
- 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 finalcertification

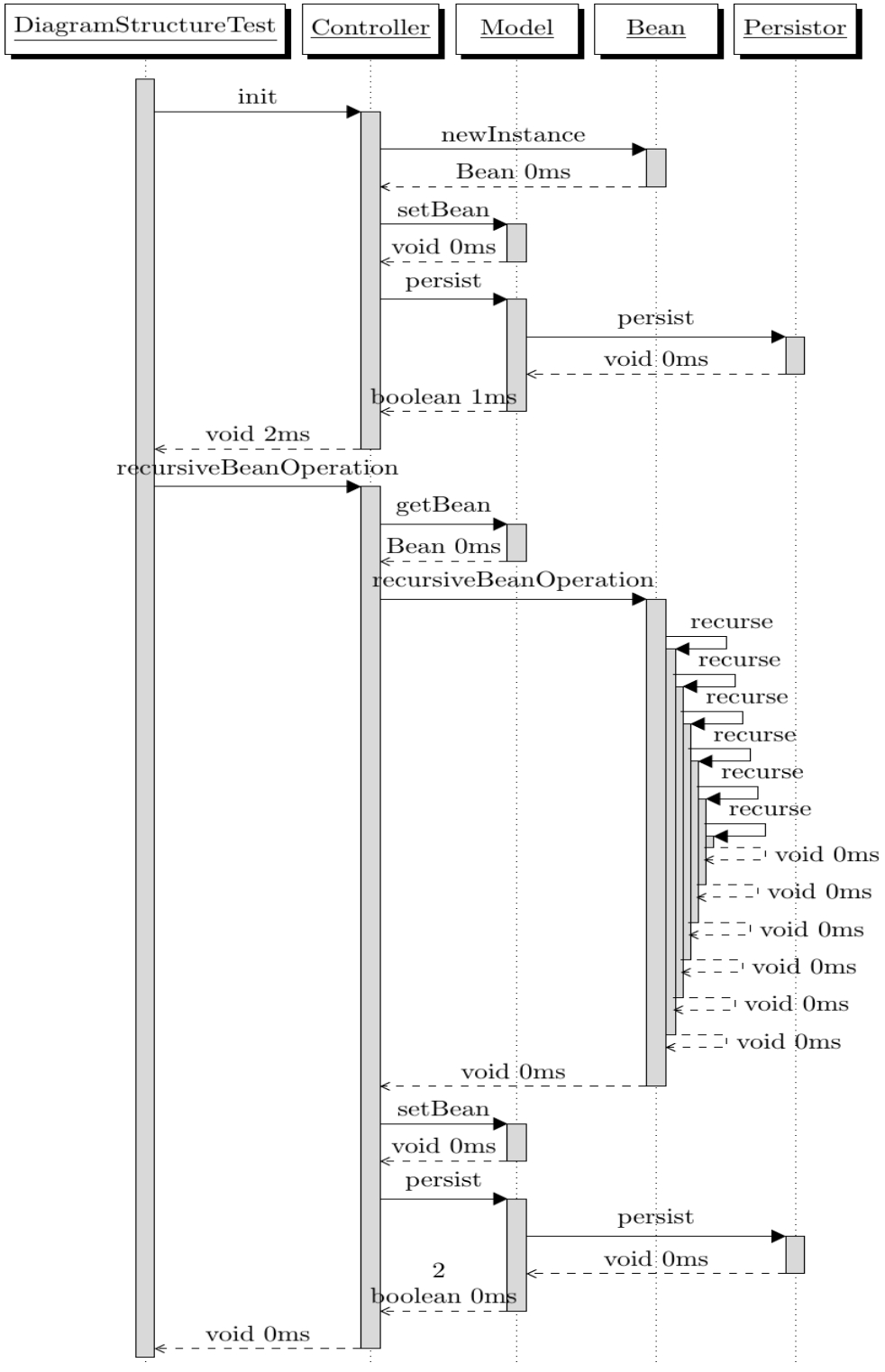
c. L0Compliance:

- Describe the software keystore implementation
  - Standard keystore used (Android, CSP, Java keystore, P12etc.)
  - Custom keystore used
    - Where is the file located?
    - File permission details
    - Keystore access rights
    - Password generationlogic
    - Passwordstrength
    - Dynamic ability inpassword

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

- 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 thesensor

Sample Sequence Diagram. - Auto generated



e. Describe the sequence diagram for "capture" functionimplementation
- Submit code for RD service and capture_sign_encrypt service (this can be part of point e above.
- Quality check, Preview, Capture Sequenceetc.
- 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 thesensor.
- Confirmthatcapture_sign_encryptserviceandkeymanagementisimplementedas native compiled code

f. Registered Device (RD) ServiceDiscovery
- Discovery of the RDservice
- Handling multiple RD services on the samehost
- Allow multiple applications talk to the same RDservice

g. ManagementServer
- Management ServerArchitecture
- Deployment and securityarchitecture
- HSM security in ManagementServer

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:

S.No	Overall
1	Entity applying for RD service certification
2	Sensor Models for RD service certification is requested (RD service may support multiple sensors)
3	Name of entity which applied for original sensor certification
4	Operating System(s) for which RD service certification is required (There will be separate installable for each OS)
5	Modality (Fingerprint / Iris)
6	Level of compliance claimed (L0/L1)
7	Diagram showing the solution architecture and all its components
8	Show that is not possible to insert a (stored) biometric into the RD service and get it signed and encrypted
9	Show that it is not possible to extract the private key of the registered device
10	Submit source code for RD service and capture, sign and encrpyt service
For L1 Compliance	
11	Provide Hardware Block Diagram with component list
12	Provide Datasheets for IC's used in the design
13	Provide internationally relevant certifications for Trusted Execution Enviroment if available

14	Describe secure boot sequence
15	Describe secure storage of keys (Valid for L0 compliance devices with hardware keystore)
16	Sequence diagram to show biometrics are signed and encrypted within the trusted execution environment.
17	Sequence diagram for key rotation
18	Sequence diagram for secure software upgrade

19	Sequence diagram for UIDAI public key update
20	Provide methodology and tools to allow certifiying agency to verify the L1 compliance for final certification
	For L0 Standard Keystore
21	Describe standard keystore used with links to description
22	Confirm that capture, sign and encrypt service is written in natively compiled code
	For L0 Custom Keystore Implementation
23	Location of Keystore File
24	File permission details
25	Keystore access rights
26	Password generation logic
27	Password strength
28	Dynamic ability in password
29	Confirm that capture, sign and encrypt service is written in natively compiled code
	Sequence Diagram for "init" Function
30	Sequence Diagram for device registration
31	Sequence diagram for key rotation
32	Sequenxe diagram for RD service update
33	Sequence diagram for UIDAI Public Key update
	Sequence Diagram for "capture" Function
34	Sequence diagram for Preview if available
35	Sequence diagram for Quality check if available
36	Sequence daigram for capture, sign and encrypt
	RD Service Discovery
37	Discovery of the RD Service
38	Multiple RD Service on same host
39	Multiple applications talking to same RD service
	Management Server
40	Management Server Architecture
41	Deployment and Security Architecture
42	HSM security in the Management Server

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 RDservice.
- Itiscertifiedthereisnodebugorbackdoormechanismtoextractthe privatekeyfromtheRDserviceand 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 L0devices.
- ItiscertifiedthattheDeviceproviderwillactivelywatchforanyknownattacksorexploitsorvulnerabilitie

s that could help an attacker extract the keys and work towards patching thesame.

- ItiscertifiedthatDeviceproviderprivatekeyissecuredusinganHSMandappropriateaccesscontroland monitoring mechanisms are in place within the management server environment to protect access to productionmachines.

- 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 andregulations.

Declarations 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 compliancedocument)

- It is certified that the TEE has a secure bootprocess

- ItiscertifiedthattheTEEsupportssecurestorageofencryptionkeysinisolatedhardwareandthesameis not exportable by any means outside of theTEE.

- It is certified that the TEE supports asymmetric key signing and encryption (RSA2048)

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

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

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

- It is certified that the environment has the capability to securely upgrade the software in theTEE

- 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 asresponse.

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. Deviceregistration/de-registration
    a. Registration of new device through init function on startup
        - Logs of managementservers
    b. Successfulauthentication
    c. De-registration of device through **backend(portal)**
    d. Auth failure due to unregistereddevice
        - 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 Keyrotation
    a. Configure management server for very short validity of devicecertificate
    b. Auth failure due to expired devicecertificate
    c. Rotate certificate throughinit
    d. Auth success after rotation; verify that new certificate wassent

3. Upgrading the RDService
    a. Authsuccess
    b. Revoke version of RD service through backend(portal)
    c. Auth failure due to wrong version of RDservice
    d. Upgrade the software version of RD service throughinit
        - Init will obtain correct version through service registryxml
    e. Auth success after RD serviceupgrade

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

5. Upgrading UIDAI PublicKey

a. Update incorrect UIDAI public key in RDservice
b. AuthFailure

c. Update correct UIDAI public key throughinit
d. Authsuccess

6. ClientFunctionality
   a. DeviceDiscovery
      i. Single RD Service
      ii. Multiple RD Services
   b. Capture call should provide the device status as per the devicesstate
      iii. READY/NOT_READY/BUSY as per the registered devicespec
   c. PreviewValidation
      iv. Sub-sampling,distortion
   d. RD servicefunctionality
      v. Optional input parameters, positive and negative testcases

7. Compliance Check
   a. Population:100residentswhoarenormallysuccessfulwithAadhaarauthenticationusingthe relevantmodality
      i. SuccessRate
         - UID level success:98%

8. Poor Quality Biometric CaptureCheck:
   a. Population: Upto 5 residents typically requiring more than one attempt to do succeed using the relevantmodality
      i. SuccessCriteria
         - UID level success: 60% success within 5attempts.

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 RDservices.

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 invalidXML.
   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 servicecalls.

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 forresponse.
- 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 thesame.

1. Insertainternetproxyandtryinsertingkeysintheresponse.Oncecompletedvalidateifacapture succeeds. Capture call should end withfailure

   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 managementserver.
   2. Try replaying the same response for a differentdevice.
   3. If a value available in the request and response then replace the values appropriately and then replay theresponse.

   Results:

   - The Device/RD service should reject the response and continue to work with this previous known configuration or should attempt moretries.
   - 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 afailure

3. Remove signature and try upgradation of unsignedfiles.

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

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 notextractable.

   Description:

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

Steps:

1. **Check the current FIPSlevel**
2. **Check the attributes of the device provider privatekeys.**

Results:

1. The FIPS level should be at a minimum of 140-2 Level2
2. HSM should have the ability to work in FIPS 140-2 Level 3 to ensure physical protection ofkyes.
3. The attributes of the device provider private keys should be marked as non exportable.

6. Perform VA and PT exercise on the serverinfrastructure

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 notrunning.
2. Only port 80 and 443 is opened for publicaccess
3. Backbone Management ports (SSH or any other) are restricted based on IP or privatekey.
4. All communication should happen only onSSL.
5. VulnerabilityScan
6. Penetration testing on the management server should beperformed.

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 (L0only)

8. Try interchanging keystores call capture, The RD service should fail (L0only)

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. (L0only)

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 keystorefile.

Attempt to break the files using rainbow table based password guess and also use all

thelist 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 thekey.

- In case there is a need for a password then try to bruteforce thepassword.

Result:

Digital signature should not succeed.

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 asDevice A) to DeviceB.
- Run capture command against the RD service of DeviceB.

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 themobile
- The keys should never be store in thekeychain.

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 roamingprofile
- 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 berestricted.
- Copy the files from device A to device B, Ensure the locations aresame.
- Once done try the capture service on deviceB.

Result:

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

11. KeyRotation

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 case11
- Force a key rotation on thedevice

- Now call the RD service captureapi.

Result:

Validate if the RD service return a valid PID.

12. Record & Investigatedata

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 keyrotation.
- Keep this information asrecord.
- Startfuzzingthecommunicationwithamixofvalidandinvaliddataforapredefined duration.
- Record all the data for futurereference.

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. Bluetoothwrangling

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 predefinedchannel.
- Active scanning for available channels should beperformed.
- Userbluesnarfing,crawlersandbluebugtoolstotestthebluetoothonknownissues and hiddenexposures.

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 MountUSB

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 ismountable.
- In windows most of the work is performed by the usbd.sysfile.
- Capturetheentirecommunicationandseeifwecanforcetheusbmountevenwhen the discover of USB mass storagefails.

Results:

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

15. Memory Dump the RDService.

Description:

Force memory dump before and after capture as the RD service and try to find if there is

aany secret hardcoded information.

Steps:

1. The latest version operating systems comes with ability to force a memorydump.
2. Use those abilities to force the memorydump

3. Takefewdumpsandanalyseusingthedumpanalysistoolsspecificforeachoperating 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 thecertificate.
2. Attempt tocapture

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 previewdisplay)

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 theextractor
3. Validate the quality of theextraction.

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 delcertcommands
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 storesecret

Steps

It's a simple test case to decompile and validate.

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

Steps

Its an audit and self certified.

21. Security ReleaseProcess

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 SigningProcess

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 publickey

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 UIDAIkey.
2. The UIDAI key validation is performed by looking for the CN names and validating CCA certificates.
3. Perform the capture call through RDservice.

Result:

The RD Service capture call should fail.

24. DNSspoofing

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. SpoofthedomainnameofmanagementserverandUIDAIserver(Theurlwherethepublic key is hosted) using the host file for the RDservice.
2. Perform the capturecall

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 listedabove

26. Look for code coverage report and validate if there are public methodsexposed.

27. ReverseLookup

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 thefunctions.
2. Validate no methods accepts biometric forsignature.

Results

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

28. FakeRegistration

Description:

Call registration service with random serial numbers and well formatted serial numbers matching the device providers serial number generation.

Steps:

1. Understand theformat.
2. Enumerate some possible serialnumbers
3. Attemptregistration.

Results:

Registration should fail.

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

Annexure – III 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 byUIDAI.
    a. TheURLs,Keysandotherparameterstobeusedinthetesting(suchasrdsId,rdsVer,dpId,mietc) would be provided by UIDAI to theprovider.
    b. Testingcanbedoneovertheinternet.TheproviderneednotcometoUIDAIorgetintoanyformal agreements while testing the Services against the PoCenvironment.
    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- RegisterAPIs.
    d. Providerwillproceedtothepre-productionenvironmentonlyaftertestingsuccessfullyinthe PoC environment.
    e. PoCenvironmentwilllatergetmergedwithStagingenvironmentandsufficientsamplecodesand test clients will be made available byUIDAI.

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 beencompletedinPoCenvironment.Theentitieswillbeentertainedinthecertificationschemeonlyafter the clearance from UIDAI. Following details are to besubmitted.

    a. SubmitacopyofSTQCcertificationofthesensorifavailable.Providershouldconfirminwritingo r provide an undertaking that the sensor has either undergone STQC accuracy certification successfullyorisintheprocessofcertification.**Incasethesensorisintheprocessofcertification , the field deployment will happen ONLY post the accuracy certification fromSTQC**

    b. Provide documentations and declarations in the provisional certification checklist get validation from STQC. This includes solution architecture with traceability matrix, declarationsetc.

    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 rdsVeraccordingly.

    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 anHSM.

3. OnceclearedbyUIDAI/STQC,theprovider&devicedetailswillbecreatedinRegisteredDevicesEcosystem and a dpId, mi will be assignedaccordingly.

4. The provisional certification functional test will be carried out in UIDAI Pre-Productionenvironment.
    a. The provider has to reach UIDAI Technology Centre, Bangalore for demonstrating the functional readiness in Pre-production, after taking a priorappointment.
    b. URLs, licence keys and other facilities to connect to the environment will be provided byUIDAI.

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

6. During the testing (onboarding phase), it is not mandatory to use an HSM, instead the keys can be stored inaUSBdongleaswell-abidingtotheCCAmandatesforcertificates.Forproductionmigration,thesame keys should be exported to an HSM or a fresh key to be procured inHSM.

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

8. Oncethefunctionaltestingandsecuritytestsarecompleted,andthereportsgeneratedaredulyvalidated bySTQC,therdsId/rdsVerwillbemigratedtoproductionandtheproductionregistryXMLwillbeupdated accordingly (only if the sensor has already completed STQC accuracy/environmentalcertification).