Procedure for Pre-Certified Hardware (PCH) Testing Evaluation and Certification

(STQC/BDCS/P09)

Issue: 01

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

Contents

0.1.Approval and Issue

This document is the property of Biometric Device Certification Scheme (BDCS) and should not be reproduced in part or full without the written consent.

Reviewed by : Management Representative

Approved by : Head, BDCS

Note:

- Management Representative 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.

2. Purpose

The purpose of this document is to define the methodology to verify the compliance of *claims made by PCH provider* with respect to latest L1 registered device specification and traceability matrix document published by UIDAI.

3. Objective

The key objective is that the PCH shall comply with the requirements as specified in the L1 Registered Device Specification and traceability matrix document for predefined TEE (Trusted Execution Environment) boundary.

PCH vendor may implement TEE on Single chip (i.e. Micro Controller, Micro Chip, Secure Processor, Secure Chip etc.) or set of chips on single PCB.

4. Reference Documents

STQC/BDCS/D01	:	Rules and Procedures
STQC/BDCS/D08	:	Specifications
ISO 27001	:	Information Security Management System
ISO/IEC 17065	:	Conformity assessment -- Requirements for bodies Certifying products, processes and services
ISO/IEC 17025	:	General Requirements for the Competence of Testing and Calibration Laboratories.

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)*

5. Definitions

Device
Fingerprint / Iris device providing final solution using Sensor, PCH and peripherals.

Device Manufacturer / OEM / Device Provider
One who manufactures the above said device and is also responsible for all the management server related services.

TEE
A Trusted Execution Environment (TEE) is an environment for executing code, in which those executing the code can have high levels of trust in that surrounding environment, because it can ignore threats from the rest of the device

Traceability Matrix:
The checklist used for ensuring compliance with claims made by device provider and/or PCH provider for a particular device/PCH.

6. Principal and Approach

To build confidence on the security of the device (L1 registered device), the overall approach is based on following principles. Since in this type of product, different functions of device manufacturing are performed by expert agencies or specialist contractors as part of supply chain, necessitating designing **assurance methodology** based on following principles:

- Use of principles of **secure product design**

  - Identify the problem context by defining security objectives and identifying security requirements in the context of L1 registered devices
  - Perform Threat modelling to identify countermeasures for secure system design
  - Incorporate System security engineering processes (NIST SP 800-160) as solution context

- **Use of Principles of demonstrating system trustworthiness:** by combination of assurance mechanism and compliances. This is a decision-making context that provides an evidence-based demonstration, through reasoning, that the system–of-interest is deemed trustworthy based upon a set of claims indicating achievement of security objectives. The trustworthiness context consists of:
  - Developing and maintaining the assurance case for fulfilment of claims to prove its truthiness and

- Demonstrating that the assurance case is satisfied. This can be done with the combination of the following techniques:

    - *“Statement of compliance and/or declarations” of device provider and PCH provider as per UIDAI requirements (L1 Registered Device Certification-Requirementsi.eL1 Traceability Matrix document and* Aadhaar Registered Devices – Technical specification*)*
      Note: The person who signs the declaration should be associated legally with the company (i.e. Director) and should have DIN number (Director Unique Id Number issued by MCA).

    - *Verification of artefacts, demonstrating compliance obtained through global certification/compliance programmes.*

    - *Demonstration of compliance by device providers and PCH providers using their procedures as test script, test jigs and other necessary tools and instrumentation which are validated.*

    - *Validations by STQC test labs or STQC recognized expert agencies.*
        - *PCH provider should provide production sample and/or an Engineering model with access probes to facilitate compliance testing.*
        - *PCH provider should provide necessary Tools, Development Kit/Engineering Board with access probes to facilitate compliance testing.*

The PCH provider shall prepare "System Security Engineering Manual" (or Technical Construction File (TCF)) which focuses on implementation mechanisms. The TCF shall define and establish problem, solution and trustworthiness contexts to ensure the security of a system, which is based on achieving a sufficiently complete understanding of the problem as defined by a set of stakeholder security objectives, security concerns, protection needs, and security requirements. This shall be evaluated using the artifacts requested in the traceability matrix.

System Approach: security control applications points in the **L1 eco system** operational environment by using information security management system processes (ISO 27001) with focus on exercising control of different entities of supply chain. This shall be evaluated using the artifacts requested in the traceability matrix.

To ensure integrity of L1 registered device services there are two essential requirements:

a) L1 device should be secure by design- criteria for which are defined in traceability matrix and derived from on Aadhaar Registered Devices Technical Specification and mapped to NIST SP 800-160 (System security engineering)

b) The service ecosystem should be secured- The criteria for which defined in traceability matrix and derived from Aadhaar Registered Devices Technical Specification and mapped to Information System Management System (ISO 27001)

The above two criteria is applicable to the whole supply chain, life cycle and major entities (Chip Supplier and device supplier)

7. Procedure

7.1.Stages of Certification:

PCH provider responsible for producing complaint PCH for UIDAI ecosystem shall follow the sound design principles and establish security assurance processes.

Following are the key stakeholders for PCH ecosystem:

- PCH provider (CPU, Secure Crypto Block/Processor, Hardware Key Store with crypto processing functionality)
  - Design (Design implementation is evaluated through solution Architecture review
  - Manufacturing (Assurance of quality and security, demonstration by QMS (ISO 9001) and ISMS (ISO 27001) compliance certificates.
    - Distribution control process through Programming (key generation) and Provisioning (Cik creation)

- PCH Provisioning Partner
  - Root of Trust establishment with Secure-Boot (firmware)
  - Chip Identity (CIk) creation (as per laid specification) generated internally and not injected via creating externally.
  - Injection of Public-Key used for signing of Device provider RD Service.
  - Cryptographic Libraries

- Testing, Quality Assurance and Release (applicable to all above categories)

These are controlled by two major certification stakeholder

- PCH Provider
- Device Provider

7.2.The certification of the PCH Provider:

The PCH provider shall identify the entities in its supply chain for design manufacturing, quality assurance and supply of chips through an entity relationship diagram highlighting the role and relationship and details of various critical entities. The number of entities could be different for different technical architectures and business models. In some cases, these entities are different specialist contractors or expert agencies and in other cases, a single agency may perform all the operations. Broadly, these specialist contractors cover different entities of the life cycle stages of concept, design & development, production, utilization, support, retirement.

The security controls exercise by PCH provider should be as per traceability matrix (PCH) and Aadhaar Registered Devices – Technical specification. Detail artefacts, demonstrating compliance, declarations etc. shall be submitted to STQC in the form of Technical Construction File (TCF).

7.3.Steps for PCH Provider Certification Process

1 PCH provider to study Aadhaar Registered Devices Technical Specification and traceability matrix in detail and ascertains that the Proposed Pre-Certified Hardware (PCH) meets the requirements submits the application (BDCS-F01).

2 PCH provider should prepare a detailed technical solution architecture demonstrating capability of PCH to meet with UIDAI objectives as per Aadhaar Registered Devices Technical Specification and Traceability matrix document.

3 Solution Architecture review by experts committee member nominated by the UIDAI and the report will be submitted to STQC for release to the vendor.

4 Certification Body will evaluate document submitted and if found prima facie worthy of the proposed technical solution architecture, may schedule detailed technical review with presentation and discussion to explain architecture and its merit.

5 The PCH provider should prepare themselves by developing secure-boot code, secure-update support, crypto library, test cases and required artifacts as defined in the traceability matrix. Ensure to follow a secure engineering process to create the PCH.

6 PCH provider shall prepare device design guidelines/instructions and provide necessary tools to be used by the device provider and this list should be part of TCF. (like tool to load device Firmware, IDE, guidelines to use Tamper protection etc)

7 PCH provider applies to STQC for PCH certification by submitting application and technical construction file (TCF). The contents of technical construction file should at least consists of

   a) The artifacts defined in the traceability matrix

   b) Artifacts to be used for test cases for verification and validation purpose. (Engineering board, demo board etc)

8 CB may allocate the application number under the scheme and same will be communicated to Test Laboratory.

   a) Based on application number, PCH vendor shall contact Test Laboratory for proposal, SRF, submission of charges and test samples.

   b) Test laboratory shall evaluate the PCH solution based on TCF submitted, Vendor shall provide necessary support as and when required by Test Laboratory.

   c) PCH provider should demonstrate testing and validation as defined under the demonstration section of the traceability matrix document.

d) Laboratory will submit the final test report including TCF review report to CB

e) Laboratory will also submit final TCF (if any change) for the TCF submitted by PCH Vendor as per traceability matrix document.

9 CB may also appoint Auditor to conduct audits for Provisioning Centre/Server, Development Centre and Programming Centre of PCH.

a) Auditors will prepare the audit report and submit to the laboratory for release to the PCH Provider.

b) Lab will submit final Audit reports along with closure action taken by PCH provider to CB.

Note: PCH provider shall provide the following to the STQC:

A conformity device (Engineering model or Golden unit or Development Kit): a device/kit with probes and access points with the necessary tools, which allows to check the implementation of the conformity document.

1. JTAG to allow direct control of chipset.
2. The JTAG device/pod/system configured as needed.
3. Give access to internal keys – a specific hardware version and configuration to allow checking of restricted areas.
4. Testing through specific interfaces that not available to ‘normal’ customers – example to read the secrets
   - UIDAI API interfaces
   - JTAG access
   - Low Level firmware interface

8. Certificate

Certification committee evaluates compliances in holistic way and integrates information from all channels stated above. Based on compliances along with Certification Committee recommendation, certificate of approval is issued to PCH provider.

The validity of the certificate will be issued for three years from date of issue subjected to surveillance audit.

Annexure-I TCF requirements for Pre-Certified Hardware

Technical Construction File (TCF) submitted by PCH vendor to BDCS Certification Body shall document:-

- Compliance/demonstration/validation to ALL applicable clauses as per L1 traceability matrix document.
- PCH Solution architecture as per latest Aadhaar Registered Devices – Technical specification published by UIDAI.