Kick off meeting on Certification of L1 Registered Devices

16/11/2018

Purpose of the Workshop

- L1 Registered Devices documentation finalized
- Certification methodology for L1 Registered Device
- Certification window open from Dec 1st, 2018

Objective & Purpose of Certification

Objective: Meet the L1 Registered Device Specification

- No mechanism for any external system to provide stored biometrics and get it signed and encrypted
- No mechanism for external system/probe to obtain device private key used for signing the biometrics

Purpose

- Verifying the compliance of *Claims made by device providers* with respect to L1 device specification requirements published by UIDAI.
- To guide the means of demonstrating compliance.
- To provide adequate degree of confidence on the security assurance of L1 Devices.
- Consideration of economy and efficiency of the certification process without compromising the required trust level.

UIDAI Registered Devices Certification

Pre-Requisites:

- Sensor testing as per UIDAI Authentication Device Specification
  - Image Quality, Environment Endurance, Electromagnetic Compatibility, Safety and ergonomics tests in laboratory environment
- Compliances based on Global Recognition (MINEX, RoHS etc.)

- Sensor accuracy performance testing in the field (FRR-False Rejection Rate)

FRR: Round IV Status

Period of exercise

23/10/18 to 24/10/18 (Dry Run)

25/10/18 to 01/11/18 (Actual Test)

Total Data Elements – 3.8 Lakh

Total Subjects participated – 5673

Received representation from participants about missing subjects, Mehandi cases, 566 Errors etc.

These are under review and cleaning in process(removing test ids, midway out, error 566 etc)

Proposed date of Test Report submission to STQC

1st week of December'18

Present Status

L0 Registered Devices Present Status

- Provisionally Certified - 101(Subject to FRR clearance- validity will be extended for 3 years)

L1 Registered Devices Present Status

- L1 specification finalized
- Assessment Methodology finalized
- Comments received from various stakeholders on traceability matrix:
- Version 0.91 is uploaded at STQC website after incorporating comments

Way Forward

Based on the consensus both documents will be released as first version after formal approval from UIDAI

Certification activity will start from **1st December 2018**

Certification will be an ongoing activity depending on vendor readiness

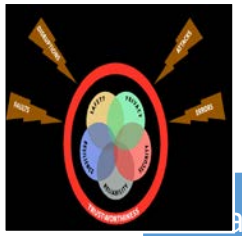
Principles and Approach

- Use of principles of **secure product design**
- **Use of Principles of demonstrating system trustworthiness**
- **System Approach**

Principles and Approach

• Secure Product Desi

evice should be secure by design
- The service ecosystem should be secured
- 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



• System Trustworthine

atement of compliance and/or declarations" by PCH and device provider as per L1 specification
- Verification of artefacts
- Validations by STQC test labs or STQC recognized expert agencies

• System Approa

to End ecosystem to be secure
- Identify entities and their relationship
- Identify applicable controls

PCH Provider Certification Process Steps

Step1: PCH provider to study UIDAI L1 registered device addendum and traceability matrix in detail and ascertains that the Proposed Pre Certified Hardware (PCH) meets the requirements.

Step 2:- PCH prepare a detailed technical solution architecture demonstrating capability of PCH to meet with UIDAI objectives as per L1 registered device addendum.

Step 3:- UIDAI technical team will evaluate submission 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.

Step 4:- 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.

Step 5:- PCH provider applies to STQC for certification by submitting application along with required fee along with TCF

PCH Provider Certification Process
Responsibility: PCH provider

Step 6:- PCH provider should demonstrate testing and validation as defined under the demonstration section of the traceability matrix

Step 7:- PCH 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)

Step 8:- Certification committee of STQC evaluates compliances. After concluding all compliances certificates of approval is issued to PCH

PCH Certification Process (Dec 2018-Feb 2019)

- Solution Architecture 1st Review (PCH). (Step 1-4)
- Documentation including third party certification, self declarations, usage guidelines, mapped to traceability matrix
- Trial demonstration including procedure and reports

- Solution Architecture Final Review (PCH) (Step 5-8)
- Final Documentation incorporating feedback from Solution Architecture
- Final Demonstration
- Code Review Report

- PCH process complete

Device Certification Process

Step 1: Application along with testing and certification fee, Technical Construction File (TCF) as per traceability matrix

Step 2: Adequacy evaluation by Expert Team

Step 3: Architecture review by expert team, Detailed Review of TCF and system security engineering manual

Step 4: Demonstration of compliances

Step 5: Demonstration of Tamper responsiveness. Applicable in case the Device Provider applies for tamper responsiveness.

Device Certification Process

Step 6: Verification and validation including RD service functional compliances & Management server security

Step 7: Preparation of evaluation report

Step 8: Independent review of evaluation report

Step 9: Granting certification of Approval

Device Certification Process (Dec 2018 - Feb 2019)

- Solution Architecture 1st Review (DP) (Step 1-3)
  - Documentation including third party certification, self declarations, mapped to traceability matrix
  - Trial demonstration including procedure and reports
- Solution Architecture Final Review (DP) (Step 4-5)
  - Incorporate feedback from Solution Architecture Committee
  - Final Demonstration
  - Code Review Report
- Functional, Security and Compliance Test Executed (Step 6-7)
  - Functional, Security and Compliance Test Report Validated by Solution Architecture Committee

Certification Charges

PCH Provider

Application Fee: Rs. 10,000

Total certification Charges : Rs. 2,50,000+18% GST

Device Provider

Application Fee: Rs. 10,000

Total certification Charges : Rs. 1,50,000+18% GST

Reference Documents

- Aadhaar Registered Devices – Technical specification version 2.0 (Revision 2), July 2017
- L1 Registered Device Addendum v1.0.
- System security engineering (NIST SP 800-160)
- ISO 27001 Information Security Management System - Requirements

Thanks