L1 Registered Device Addendum v1.0

This document speaks about the key objectives, evaluation criteria and certification process for a device provider who applies for a L1 certification. The requirements for an L1 certification are in addition to the functional requirement for L0 certification. The device provider needs to read this document in conjunction with the Aadhaar Registered Device Specification 2.0: https://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_09112016.pdf

This documents supersedes any other document related to the certification of L1 devices.

Registered devices MUST ensure the following

Objective 1. There should be no mechanism for any external system to provide stored biometrics and get it signed and encrypted.

Objective 2. There should be no mechanism for external system/probe to obtain device private key used for signing the biometrics.

1. L1 Compliance Requirements

The registered device specification 2.0 revision 1 defined L1 compliance as:

“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.”

UIDAI is further clarifying the requirement for L1 compliance in this document.

All of the processes related to create a biometric PID block must be executed within a TEE (at a level below the host OS):

1. Biometric capture
2. Biometric processing/extraction to create the bio element
3. Signing the bio element.
4. Encryption of the PID block

The following processes MUST take place within a hardware keystore (secure crypto block)

1. Identity of the chip C_k (look at section Pre-Certified Hardware Identity) should be stored in the secure crypto block and should be non clonable
2. Key pair generation
3. Signing the bio element

It is required to minimize the attack surface at the system level by using methods such as but not limited to hidden traces, protective meshing, encrypted communication etc. Minimizing the attack surface is inline with the objective 1 of this document.

In addition, it is highly recommended that tamper responsiveness be implemented for the system. UIDAI will differentiate between devices with and without tamper responsiveness.

2. L1 Certification Steps

The certification of L1 registered device consists of the following steps

1. “Pre-certified” hardware (PCH) validation by UIDAI/STQC
    a. Secure crypto block with international certifications
    b. TEE certification as defined in section 4 of this document.
    c. Secure provisioning process

2. L1 compliant registered device solution architecture validation by UIDAI/STQC using “pre-certified” hardware
    a. Secure system design inline with the key objectives of the UIDAI RD Service specification (latest version)

    b. Implementation of RD Service and Management Client inline with RD Service Specification (latest version)

3. STQC certification process
    a. Functional test - Similar to L0 certification
    b. Compliance test - Similar to L0 certification
    c. FRR test - Similar to L0 certification
    d. Security test. - Combines L0 and L1
    e. Demonstration of system level tamper responsiveness (if applying for tamper responsiveness)

3. L1 Device Threats:

The following set of threats are expected to be addressed as a part of the L1 device solution architecture. Its expected that the pre-certified hardware provider would provide documentation to support the solutions claims on mitigating these attacks. The mitigation techniques if listed in this document are standard choices and vendors may implement other techniques to mitigate threats.

A. “Pre-certified” hardware (PCH), system software threats

The Pre-Certified hardware, system software should protect against the following threats.

1. Hardware cloning attack
2. Hardware Tamper attacks
    a. Physical tamper, etching, chemical tampering , voltage, frequency, temperature attacks on crypto block
3. Differential Power analysis attack
4. Probing attacks
5. Cryptoprocessor to external memory communication
6. Segregation of memory for execution of cryptographic operation
7. Vulnerability of the cryptographic algorithm implementation
8. Attacks against secure boot & secure upgrade
9. TEE/Secure processor OS attacks

B. L1 Registered Device System Level threats

1. Probing attacks: Connectivity from the sensor to pre-certified hardware
   One or more of the following mitigations may bef implemented to achieve the tamper responsive at the system level, i.e keys must be erased if a tamper is detected.

    a. Protective mesh
    b. Encrypted channel with trusted keys between sensor and pre-certified hardware
    c. Minimize exposed surface between sensor and the pre-certified hardware

2. Software protocol attacks
   All of the following mitigations must be implemented for a L1 certification.
    a. Host to device communication channel buffer overflow/stack overflow attack
    b. Forcible software updates for security vulnerability
    c. Minimize the protocol usage to the following
        i. Capture, Device Info, Key rotation, Time Sync, Upgrade, Register, Update UIDAI certificate
    d. Declare any other functions implemented

4. “Pre-certified” hardware, system software certifications/validations:

The following certifications will be used for hardware, system software “pre-certification”

1. Secure crypto block hardware certifications may use ONE of the following certifications
    a. FIPS 140-2 Level 2 (tamper evidence) FIPS 140-2 Level 3 (Tamper resistance) - This covers hardware and software and all form of attacks.
    b. PCI - PTS v4.1 and above Pre-Certified - This covers both physical tampering and software
    c. PCI - PED 2.0 Pre-Certification and above
    d. One of following Common Criteria (CC) certification or equivalent custom profiles at level EAL4 and above
        i. https://www.commoncriteriaportal.org/files/ppfiles/pp0035a.pdf
        ii. https://www.commoncriteriaportal.org/files/ppfiles/pp0084a_pdf.pdf
2. Cryptography Algorithm Certifications:
    a. CAVP validation (If not covered in the above certifications)
        i. RSA, AES, SHA-256 (Running on secure cryptoprocessor)
        ii. TRNG Certification (DRBGVS or equivalent)
    b. FIPS 140-2 Level 1 (only for cryptography algorithm if not covered in the above certifications)
        i. RSA, AES and SHA-256
        ii. TRNG Certification
3. Self Certification:(if the design does not have a certified secure element)
    a. Certification or detailed documentation and lab reports about the implementation of “protection of side channel attacks for cryptography operations”.
    b. Self certification that the solution ensure to zero (or any other technique to ensure that the data can not be recovered) the all used memory upon a tamper attempts during the ON state.

    c. Self certification that the PCH does not store unencrypted keys in non volatile memory at any time.

4. TEE certification.
    a. Global platform certified TEE is required in the case of shared hardware i.e the processor used for purposes other L1 Registered device functionality
    b. In the case of dedicated hardwares for L1, proving secure boot, secure upgrade and isolation of access to the secure crypto block is required for the purpose of L1 certification. The following test cases should be demonstrated (if not included in the third-party international certification) for “pre-certification” on a development board including all hardware (except the biometric sensor):

        i. Secure boot
            - Should check for the integrity of the hardware platform upon every boot. The hardware configuration should be identical from the time of provisioning or first boot.
            - Should validate the signature of the image upon every boot.

        ii. Secure upgrade of OS/crypto block
            - Has to ensure that failure of upgrade should rollback to previous known cryptographically verified boot image
            - Forced upgrade in case of vulnerability detection

        iii. Secure Upgrade of Device Provider Application

5. Identity for Pre-Certified Hardware:

Identifying a pre-certified hardware uniquely is one of the key part of the L1 compliance. The following section describes the compliance needed to inject the identity into the secure crypto-block. The device identity is strongly tied to the cryptoprocessor to ensure non-clonability.

1. The identity is based on a RSA 2048 bit key pair generated within the secure crypto block and the public key is signed by pre-certified hardware provider (at the pre-certified hardware provider or at programming house working with the pre-certified hardware provider).

2. The identity should be a permanent (or one time programmable) information and the chip should live and die with one single identity. The identity is created and stored in the secure crypto block and should not be alterable or clonable by any adversaries.

3. The identity of the pre-certified hardware is as described below.
    a. A unique RSA 2048 bit key pair and a CSR is generated CI$_k$.
    b. The CSR used to issue a chip identity (x509 certificate) the root key would be same as the pre-certified provider’s root of trust.
    c. The pre-certified hardware would have a mechanism to sign using the identity key upon a external challenge.

4. No other identity keys should be present in the pre-certified hardware at this stage other than the pre-certified hardware identity key

5. Root of trust for the pre-certified hardware and device provider root should be provisioned on Read Only Memory (ROM) or One Time Programmable (OTP) memory

6. All the keys used during the identity injection process should be stored in a FIPS 140-2 Level 3 device and its the responsibility of the PCH vendor to ensure safety of these keys.

6. Secure Boot and Secure Upgrade

The device should have the ability to boot and upgrade securely. The following points would describe the minimum compliance for the same.

1. All software loaded to the device/chip should be be verifiable with cryptographically safe hash (SHA256) and signatures.
2. The root of trust for all signatures (both device provider and pre-certified hardware vendor) would be uploaded during the Key injection process.
3. All boot sequence should check for the integrity of the softwares using the respective provider keys.
    a. Upon 10 (10 is the max limit and vendors can choose a lower threshold) failed attempts to boot the device all device software, data, keys used for pairing and keys used for biometric signing, any other license keys used by the device provider should be deleted. However keys related to chip identity, root of trust etc. on a need not be deleted on optional basis. This state is considered as a tampered state of the device. In case of tampered state, field upgrade should not be possible, it must be re-programmed in the factory. (device provider must demonstrate secure method for reprogramming)
    b. Upgrade of firmware will always validate the root of trust & should move upward in version number. So firmware downgrade should be impossible.
4. Upgrades should be atomic in nature that it either happens or fails. The system can not be booted in a partially upgraded state.
5. In the event of failure in upgrade, the secure boot should re-validate the signatures.

7. Secure Provisioning

1. The facility should preferably be in India and auditable upon need.
2. The key injection should happen over a secured facility and no users should have access to, influence or steal the identity.

3. The provisioning should happen over secure & encrypted channel with minimum of 2048 bit of RSA or equivalent (more) PKI & a FIPS 140-2 Level 3 device.
    a. CI_k Should be created/injected during this process
    b. The root of trust of the pre-certified hardware and root of trust of device provider should be injected in Read only / OTP memory
    c. The secure boot manager is loaded
4. All debug options should be blocked on the pre-certified hardware before provisioning of the keys.

8. Hardware/System Software Vendor Self Certification:

1. No backdoors or debug mode enabled on the secure crypto-block
2. Documents/certifications submitted are valid for the current model of secure crypto-block.
3. The secure provisioning process is in compliance with global security standards and UIDAI specification
4. The solution architecture submitted by the device provider is inline with the security guidelines recommended by the pre-certified hardware provider
5. System level tamper responsiveness implementation by the device provider has been validated (if applicable)

9. System Level Tamper Responsiveness Certification

It is required to minimize the attack surface at the system level by using methods such as but not limited to hidden traces, protective meshing, encrypted communication etc. Minimizing the attack surface is inline with the objective 1 of this document.

If certification for tamper responsiveness is requested the vendor must submit the various tamper responsive measures implemented.

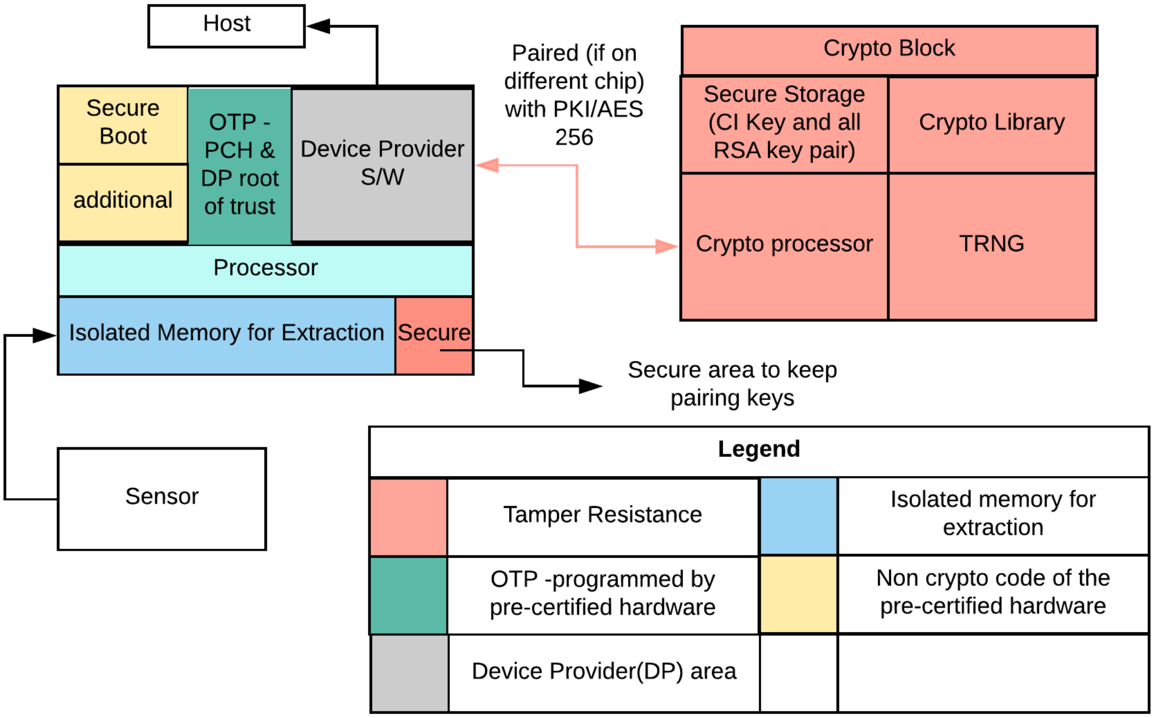
1. Review the design to understand approach to system level tamper including some or all of the following mitigations
    a. Protective Meshing
    b. Box open Tamper
    c. Pairing based Tamper Responsiveness
    d. Chemical tamper responsiveness

2. Test Cases to demonstrate the Tamper Responsiveness. PCI PED compliance test can be used as a guideline. PCI PED compliance certification is not expected.

UIDAI/STQC will differentiate between devices with and without tamper responsiveness in the certification process.

10. Reference Design for L1

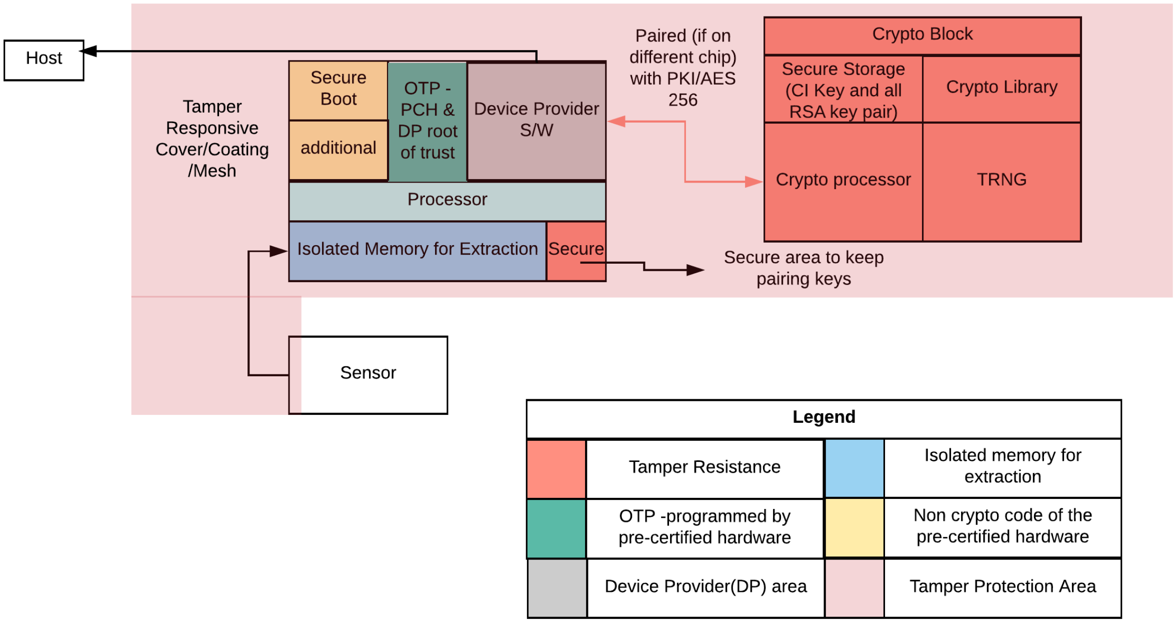
a. L1 without system level tamper



Host
Secure Boot
additional
OTP - PCH & DP root of trust
Device Provider S/W
Processor
Isolated Memory for Extraction
Secure
Sensor
Paired (if on different chip) with PKI/AES 256
Crypto Block
Secure Storage (CI Key and all RSA key pair)
Crypto Library
Crypto processor
TRNG
Secure area to keep pairing keys
Legend
Tamper Resistance
Isolated memory for extraction
OTP -programmed by pre-certified hardware
Non crypto code of the pre-certified hardware
Device Provider(DP) area

Reference Design for L1 without System Level Tamper

b. L1 with system Level tamper


Host
Tamper Responsive Cover/Coating /Mesh
Secure Boot
additional
OTP - PCH & DP root of trust
Device Provider S/W
Processor
Isolated Memory for Extraction
Secure
Sensor
Paired (if on different chip) with PKI/AES 256
Crypto Block
Secure Storage (CI Key and all RSA key pair)
Crypto Library
Crypto processor
TRNG
Secure area to keep pairing keys
Legend
Tamper Resistance
Isolated memory for extraction
OTP -programmed by pre-certified hardware
Non crypto code of the pre-certified hardware
Device Provider(DP) area
Tamper Protection Area

Reference design for L1 with System Level Tamper

Note: The diagrams are for logical illustrations and the actual implementation would be different. The images are in 2D and the protection has to be applied on a 3D object.

11. Device Identity

The device Identity has to be implemented in a specific manner for L1 devices as described below. **This definition overrides the definition of idHash in the Registered Device specification 2.0**

1. The CI_K key from the pre-certified hardware is used to “sign” the device identity.
2. The device identity data would be computed as follows:
    a. The device provider software should use the device serial number and timestamp as input (should match the timestamp value of PID) to construct the string TD.
        i. TD = deviceSerialNumber:base64(<deviceSerialNumber>);timestamp:<timestamp>
    b. The device provider will construct the idHash in the following manner:
        i. Sign1 = DigSign(TD) (signed using the pre-certified hardware sign method)
        ii. idHash=concat <deviceSerialNumber> + _##_ + <base64(Sign1)>.

    Note: _##_ is a delimiter string.

    Note: Max serial number would be 20 characters

3. The resultant idHash would be provided as idHash to the PID block for all L1 device. **Unlike L0 the idHash here is expected to change for every auth call.**
4. The management server should validate the signature in the idHash before registration and before key rotation. The idHash data has to be kept as a audit record for future verification and compliance needs.
5. The management server and the TEE software should have the ability to synchronize time a minimum once a day and host time should not be trusted.
6. The deviceSerialNumber in the idHash computation should not change for lifetime while the signature depends on the timestamp.