Akraino Platform Security Questionnaire

February 2021

Daniil Egranov, Arm

Chip Assessment Questionnaire

- This applies to the hardware and firmware that comprise the Platform Security RoT that forms the Secure Processing Environment (SPE).
- This questionnaire provides assessment for the platform security components based on Immutable Platform Root of Trust and Platform Security Root of Trust.

AKRAINO

Immutable Platform Root of Trust

1. **The chip shall support a hardware mechanism(s) to isolate the Secure Processing Environment (SPE) from the Non-secure Processing Environment (NSPE).**

(Describe how isolation is implemented, for example through TrustZone or dual cores.) Example of response for Yes: The Cortex-M33 (ARMv8-M architecture) supports TrustZone. The Secure Processing Environment is executed in secure mode.

Immutable Platform Root of Trust (Continue)

2. **The chip shall support Secure Boot, initiated from code in the immutable Platform Root of Trust. Note: that asymmetric signing is expected, however, symmetric signing can be accepted.**

(Describe which cryptographic functions and key sizes are used for secure boot, and how the cryptography is implemented, such as use of a hardware cryptographic accelerator or software in immutable code. Also describe how the Immutable code is implemented and if in some form updateable on-chip memory (such as EEPROM or Flash) how that is locked.) Example of response for Part: The initial Bootloader is run from Boot ROM in secure mode but without prior validation. This Bootloader authenticates the SPE image by hash (SHA-256) and digital signature (RSA-3076) validation. Public key is built into the bootloader image. Metadata of the image is delivered together with the image itself in a header and trailer section. In case of successful authentication, bootloader passes execution to the SPE image.

Immutable Platform Root of Trust (Continue)

3. **(Optional) The chip shall support a security lifecycle, i.e. protecting critical security parameters and sensitive data based on device lifecycle state and enforcing the rules for transition between states. Lifecycle states can typically be classed as follows, i) non-secure assembly and test, ii) provisioning, secured provisioned and operational, iii) decommissioned, and iv) debug, if debug of a secured provisioned device is supported.**

(Describe supported lifecycle states and transition rules)

Immutable Platform Root of Trust (Continue)

4. **The chip shall support the storage or derivation of following minimum set (or equivalent) of critical security parameters, in such a way that prevents unauthorized reading and resists tampering by means such as physical, electrical or software (such as external probing of the chip for confidential data):**
   - **A secret Hardware Unique Key (HUK), with at least with 128-bits of entropy, used for deriving other device secrets**
   - **A Platform RoT Public Key, or hash of, used for authenticating the first updateable firmware component code during secure boot. If symmetric signing is unavoidable, the key must be unique per device.**
   - **A secret attestation key and identifier that uniquely identifies the attestation key**
   - **An identifier that uniquely identifies the Platform Security RoT on the chip.**

   These keys and identifiers may be injected during chip manufacture or during the manufacture of the device or derived from the HUK. They can also be derived from a Physically Unique Function (PUF).

(Describe key size for each key, and if applicable the key derivation method for the Attestation Key. If HUK is derived from a PUF, provide a rationale of key uniqueness. Describe the protection of the functions to read the keys. Also describe how the chip data are protected from tampering.)

Platform Security Root of Trust

1. **The Platform Security RoT shall support secure update of firmware and any of Application RoTs. Updates may be delivered either from locally connected devices (such as removable media) or from remote servers. Updates shall be validated by the Platform Security RoT to check integrity and authenticity prior to execution (see .1 in Immutable Platform Root of Trust section) and, optionally, before installation. This includes the executable code and any related data, such as configuration data or a manifest. The cryptography used shall comply with requirements (updates (see .4 in Platform Security RoT section)).**

(Describe how updates are validated, including the cryptographic algorithms, the key size and where the keys used for validation are stored. Justification is required if local validation of update from remote servers prior to installation cannot be supported, typically due to resource constraints.)

Platform Security Root of Trust (Continue)

3. **The update mechanism shall prevent unauthorized rollback of updates (see .1 in Platform Security RoT section) and protect the current reference firmware version number in an anti-rollback counter, in secure storage (for example, protected flash or OTP). A mechanism may be provided to support authorized rollback for recovery reasons. Anti-rollback is strongly recommended but not mandatory in PSA.**

(Describe the versioning information used to detect rollback and how it is protected in integrity and against rollback and over or underflow. If supported, describe how authorized rollback is implemented.)

Platform Security Root of Trust (Continue)

4. **The Platform Security RoT shall perform access control for modification and use of Platform Security RoT critical security parameters and for System software or Device sensitive data managed by the Platform Security RoT. For example, the Platform Security RoT shall control access to any such data stored in a protected flash region or in OTP.**

(Describe the System software subjects concerned by access control and how they are identified or authenticated)

Platform Security Root of Trust (Continue)

5. **The Platform Security RoT shall use best practice cryptography for protection of its assets, as recommended for instance by national security agencies. This includes the provision of a suitable source of random data. There should be no reliance on proprietary cryptographic algorithms or customization of standard cryptographic algorithms. Platform Security requires equivalence of at least 128-bit security. NB: Weak cryptographic algorithms or key sizes may be available for specific uses (e.g. legacy) and with specific guidance. They shall not be used in any way that reduces the security of the best practice cryptography. A TRNG or a suitably seeded Deterministic Random Bit Generator can be used.**

(List the cryptographic algorithms provided by the Platform Security RoT and the supported key sizes. Also describe how random number generation is performed.)

Questions