Primus HSM – Key Attestation

Trusted and scalable verification of keys and timestamps

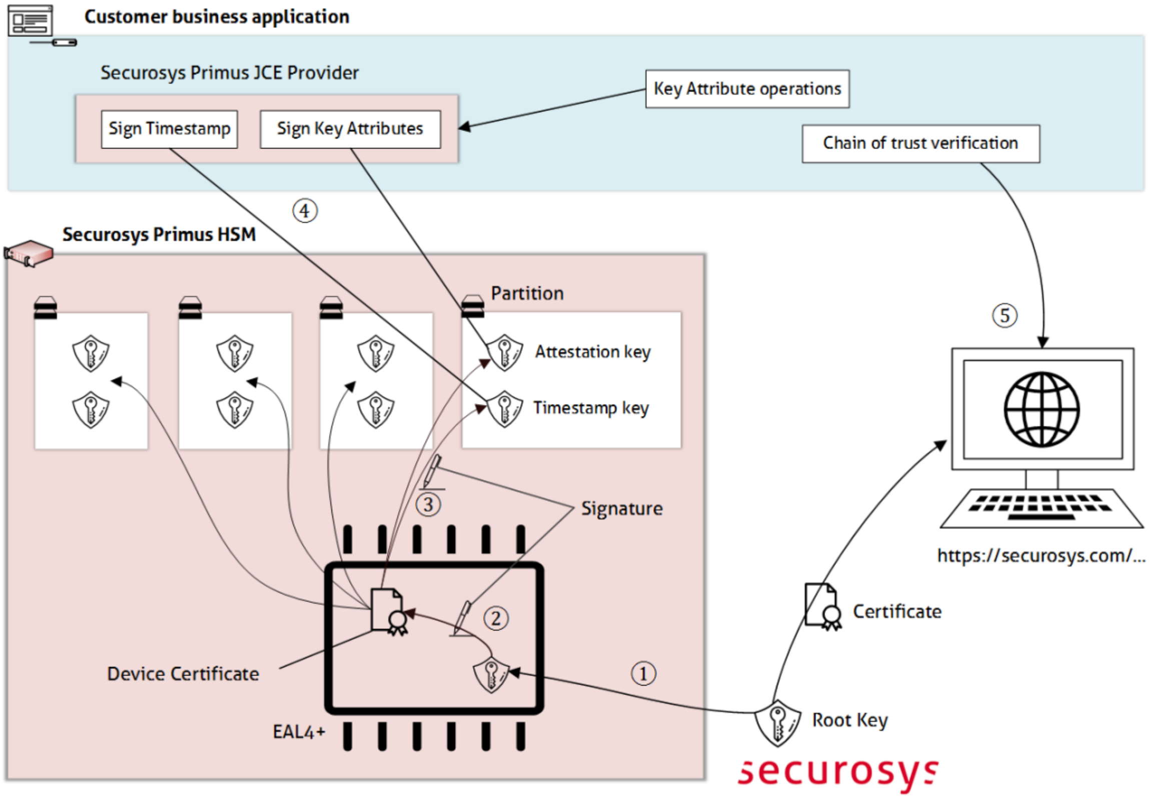
Key Attestation significantly reduces the costs of public certificate key ceremony and key distribution and massively increases scale of digital identity applications

Summary

Digital identity applications in need of qualified certificates and signatures must have the certificate keys issued in a trusted way. The way to do it currently is to have their key ceremony procedures audited and the audit approved by the certification authority. The identity keys then need to be distributed securely. All of this is costly and unscalable, and requires trust, that the audited process is applied consistently on all newly generated keys.

The new Securosys Key Attestation feature provides cryptographic verification of the key and its attributes with a chain of trust originating from our root certificate. This allows to automate the key ceremony audit process, and to issue trusted digital identity keys at virtually limitless scale.

Details



Each Primus HSM is equipped with a EAL4+ certified keystore, protecting a factory installed root (1) certificate and root key. The device then creates its own intermediary (device) key and its certificate is signed by the root key (2). The intermediary key is then used to sign attestation and timestamp key created for each partition (3). The attestation key is used to verify the key origin (i.e. that a new key has been generated on the particular HSM) and key attributes, and the timestamp key is used for generating qualified signatures or for the applications of time-based key attributes (4).

The root certificate is available at our website and its hash at our support portal, allowing any user to verify and audit the chain of certificates (5).

This way, the digital identity applications can automatically generate identities for users or devices, and verify qualified signatures with those identities without a necessity to employ additional procedures or external authorities while guaranteeing their origin and hardware protection and at a virtually zero marginal costs and a limitless scale needed for IoT and personal identity applications.

Root Key Store license is necessary to enable the feature.

Getting Started

The use this capability, follow the steps in the order below:

1) Obtain license to use the root key feature
2) Make sure the HSM firmware is of version > 2.7.6
3) Install RootKey applet

   Important: this rewrites any previous intermediate keystore.

   - On HSM: SYSTEM → ROOT KEY ELEMENT → INSTALL RKS/RNG
   - In Console: hsm_sec_install_rke
4) Create the Intermediate Key
   - On HSM: SYSTEM → ROOT KEY ELEMENT → SETUP RKS
   - In Console: hsm_sec_setup_rks
5) Create attestation and/or timestamp key for the partition:
   - For more information, refer to functions *createAttestationKey* and *createTimestampKey* in the Javadoc

About Securosys Primus HSM Series

- Scalable and flexible solution
  - X-Series (high performance)
  - E-Series (price-performance)
  - Clouds HSM (as a service)
- Secure Remote Control with Decanus
- Multi-tenancy, up to 120 partitions, each 240MB
- Strict authentication, 4 eyes principle, 2 factor auth.
- Clustering, secure “real-time” synch. across data centers
- Constant tamper protection
- Designed, developed, and manufactured in Switzerland