Personal Network HSM

www.ethertrust.com

Our society is becoming increasingly digital, underscoring the need for securing access, transactions, and data. Encryption including cryptographic operations, key storage and management are becoming vital components of a digital security infrastructure along with secure storage and tamper resistant computing. Secure applications typically use cryptographic resources such as secret keys for signature procedures or cryptogram generation and verification. For example crypto currencies hot wallets store private keys associated to blockchain accounts, and sign transactions performing crypto money transfers or smart contract calls.

Whether on premise or in the cloud, these two secure storage and computing technologies are often being used: Hardware Security Module (HSM) and Confidential Computing solutions:

- An HSM is a secure tamper-proof electronic board with a dedicated operating system, running an implementation of PKCS11 API, which creates and manipulates cryptographic tokens. FIPS140 standards specify that an accredited security officer initializes HSM and user partitions.

- Confidential computing (for example *Azure confidential computing*) runs software in isolated environment, always using encrypted data.

HSM access control relies on user PIN (usually 32 bytes). There is no standardized network interfaces for HSM; protocols such as SSH or TLS are used for remote access. In confidential computing secure channel, typically TLS, enables software updates and remote administration; trust between service provider and the computing platform, relies on the attestation procedure.

We believe that enterprise needs to store security tokens in the cloud are rapidly extending to individual consumers, beginning with cryptocurrencies account keys. Our vision for Ethertrust *Personal Network HSM* is to enable individuals to have their own cost effective personal on-line secure storage and computing service with the same trust level as the smartcards they carry with them.

- Personal means single service tenant, i.e. no shared HSM partition or shared confidential virtual machine.

- Network means having a native TLS “network” interface.

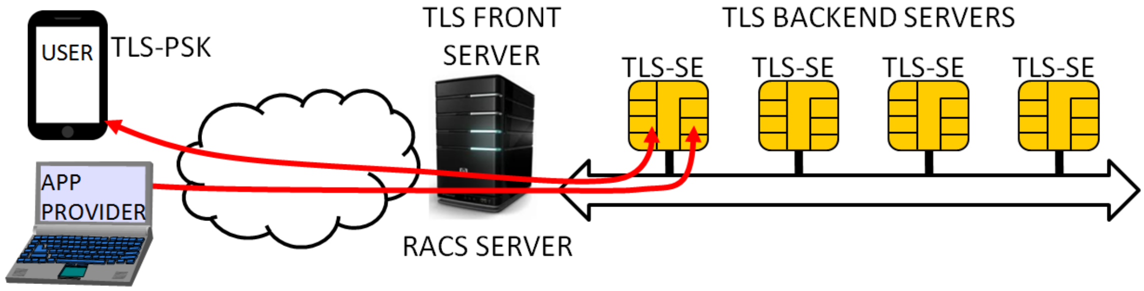
- HSM means offering through secure elements hosted in dedicated servers, the same or better FIPS accredited security than HSMs.

Almost 10 Billions of secure elements are produced worldwide annually, making it a cheap yet extremely secure storage and computing resource. A secure element based cloud service can achieve several orders of magnitude price reduction, meeting individual consumer budgets.

Personal HSM architectural considerations:

Ethertrust Personal HSM interacts with two entities: application provider and user. The application provider downloads security middleware in secure element over TLS. From the user point of view, the secure element acts as personal internet server. Trust between user and embedded app relies on a dedicated attestation procedure.

Secure elements are small chips with high security level, up to EAL6+ according to common criteria standards; they are deployed in bank cards, SIM modules, or electronic passports. Ethertrust uses the open TLS-SE technology, i.e. TLS1.3 server for secure element, using pre-shared-key (PSK) authentication.



Secure elements are hosted in grids, providing two TCP daemons, RACS and TLS, facilitating scaling.

RACS (Remote APDU Call Secure) performs secure software updates by transporting GlobalPlatform protocols over TLS. There are two security levels: Symmetric secret shared between secure element and application provider; X509 certificate to identify the application provider within TLS.

TLS front server routes TLS packets to/from secure elements backend servers, identified by their server names.

The attestation procedure relies on the fact that secure element cannot be cloned, and that they can only manage a single TLS session at a given time for stronger security.

Personal Network HSM benefits

Secure elements have the highest security level for hardware components. They are also manufactured be several companies, trust doesn’t rely on proprietary technology, as the case with legacy HSMs and Confidential Computing.

Software typically written in javacard language enables a rich ecosystem, including open source, for application providers. There is no dedicated model such as in legacy HSMs’ PKC11.

Native network interface and de facto standard for security protocol facilitate the design of comprehensive trust models.

In summary, Ethertrust Personal Network HSM, based on open hardware and software, is a very effective solution to secure on-line individual assets.