securosys

Securosys Transaction Security Broker

Unique security and developer experience for crypto-asset applications

Introduction

Not only are Securosys Hardware Security Modules (HSMs) - like older HSMs - optimized for the physical protection of private key material; Securosys HSMs provide control over the keys' usage with specific and sophisticated authorization which is essential to crypto-assets protection. *Smart Key Attributes (SKA)* allow fine-grained policies to be defined for various actions, with the keys based on groups, quorums and time restrictions, and any combination thereof.

As highlighted in Securosys' whitepaper about safeguarding of crypto-assets, this control, combined with other capabilities of Securosys Hardware Security Modules, provides protection of the assets superior to that of the traditional Multi-signature or secure Multi-Party Computation.

Securosys *Transaction Security Broker (TSB)* makes implementing the SKAs much easier thanks to its REST API and internal state management. It runs as a standalone engine, connects to an external database instance and integrates the SKA-enabled Securosys HSM, so it is not security critical as all security-related operations take place in the HSM.

Details

The TSB integrated with SKA-enabled Securosys HSM provides fine-grained control over the key actions and operations. It allows the crypto organization to set highly customizable policies for authorizing operations, blocking or unblocking the keys, as well as for changing the policies themselves. The use-cases range from *n* to *m* quorums, time-locks that enable systems to trigger alarms and block the key operations, to time-outs that ensure no suspended transaction request can be misused in the future, and any combination of these. Approval can be done on a mobile, desktop or physical cryptographic device and can also be protected by the HSM's keys.

Approval process

The approval process typically looks as follows:

1) Approval is requested to sign a cryptocurrency transaction
2) The HSM checks key attributes and sends the approval policies back to the TSB along with the payload and timestamp signature
3) The TSB and the business application broadcast the approval request to all clients in the approval group
4) The TSB waits for the approvals until the policy is met, then sends the required approval data together with the payload to the HSM
5) The HSM checks the authorization data against the key attributes (SKA), the specific payload, and optionally the signed timestamp
6) If the criteria are met, the HSM signs the payload and returns the signature

Advantages of TSB compared to Multi-Signature

- Algorithm independent - the same process can be used for all supported crypto assets and currencies regardless whether they support multi-signature or not
- Lower fees and better privacy because the addresses are single signature type
- Regulatory and customer flexibility thanks to decoupling of ownership and control of the keys
- Customizable compliance from simple to highly complex policies including time-restrictions

Advantages compared to Multi-Party Computation (MPC)

- Time-based policies
- Hardware tamper protection of the key material
- Redundancy without introduction of an additional risk of key exposure

Policies

Policies are a set of one or multiple rules. The following authorization rules can be defined as follows:

- Quorum - *n* out of *m* authorization is required
- Delay - the minimum time between the receipt of the authorization requests by the HSM and the actual signing of the payload
- Time-out - the maximum time span between the submission of the request and its authorization

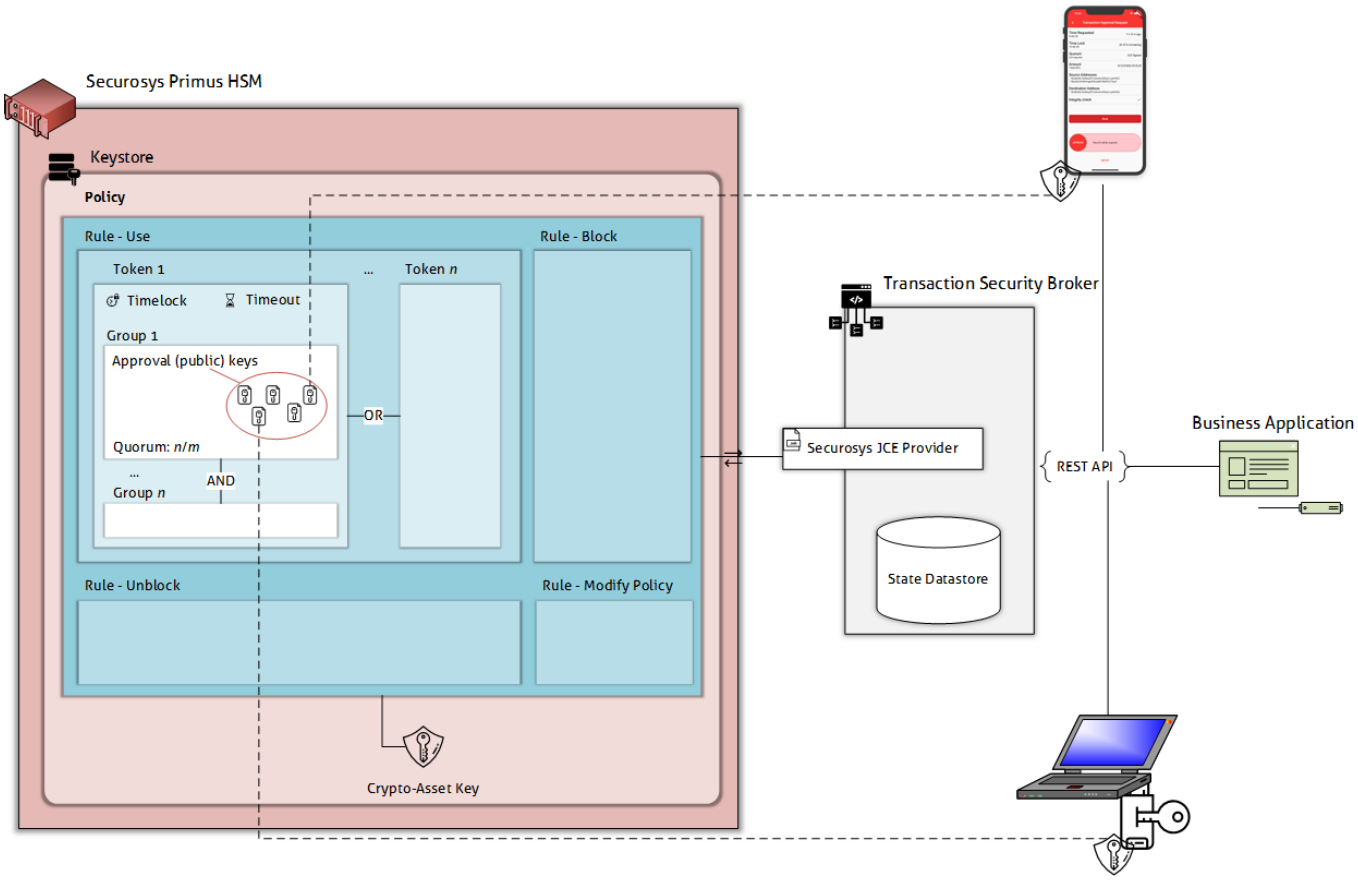
There can be multiple rules for each key, allowing various authorization levels to be customized for each key.

In addition, different rules may apply to different operations with the key:

- Usage (e.g. signature, encryption)
- Key blocking
- Key unblocking
- Change of the attributes (policies)

All of the rules can be combined and assigned down to the individual key.

Architecture



The *Transaction Security Broker* is not a standalone product but requires Primus HSM and the corresponding license.