



# ***Key management system with HSM***

***Vítor Neto***

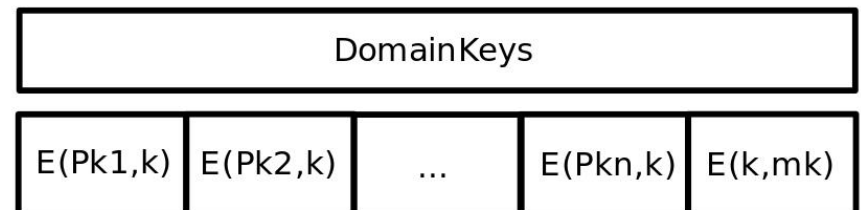
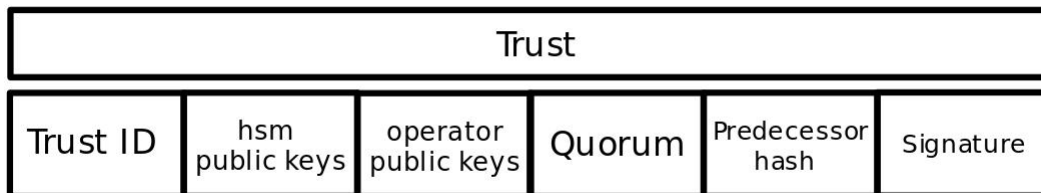
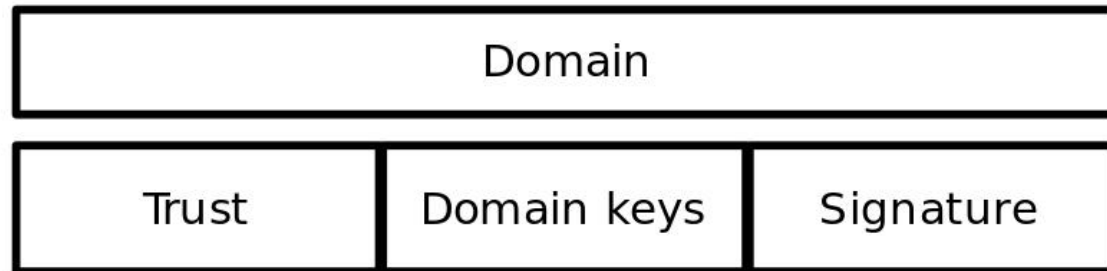
# Requirements

- *Secure storage;*
- *Integrity assurances;*
- *Accountability;*
- *Secure cryptographic key generation;*
- *Secure cryptographic operations;*
- *Secure cryptographic key storage;*

# Hardware security modules

- *Secure hardware, tamper resistance;*
- *Wide range cryptographic capabilities;*
- *Generate, store, protect cryptographic keys;*
- *High quality random number generation capabilities;*
- *Compliance;*
- *High performance;*
- *Scalable;*

# PoC – Data structures



# PoC – Architecture

