Sign Hyperledger Fabric Smart Contract using the TPM

Student: Zeddrich Starke (z.n.starke@student.tudelft.nl) , Responsible Professor/Supervisor: Kaitai Liang (kaitai.liang@tudelt.nl)

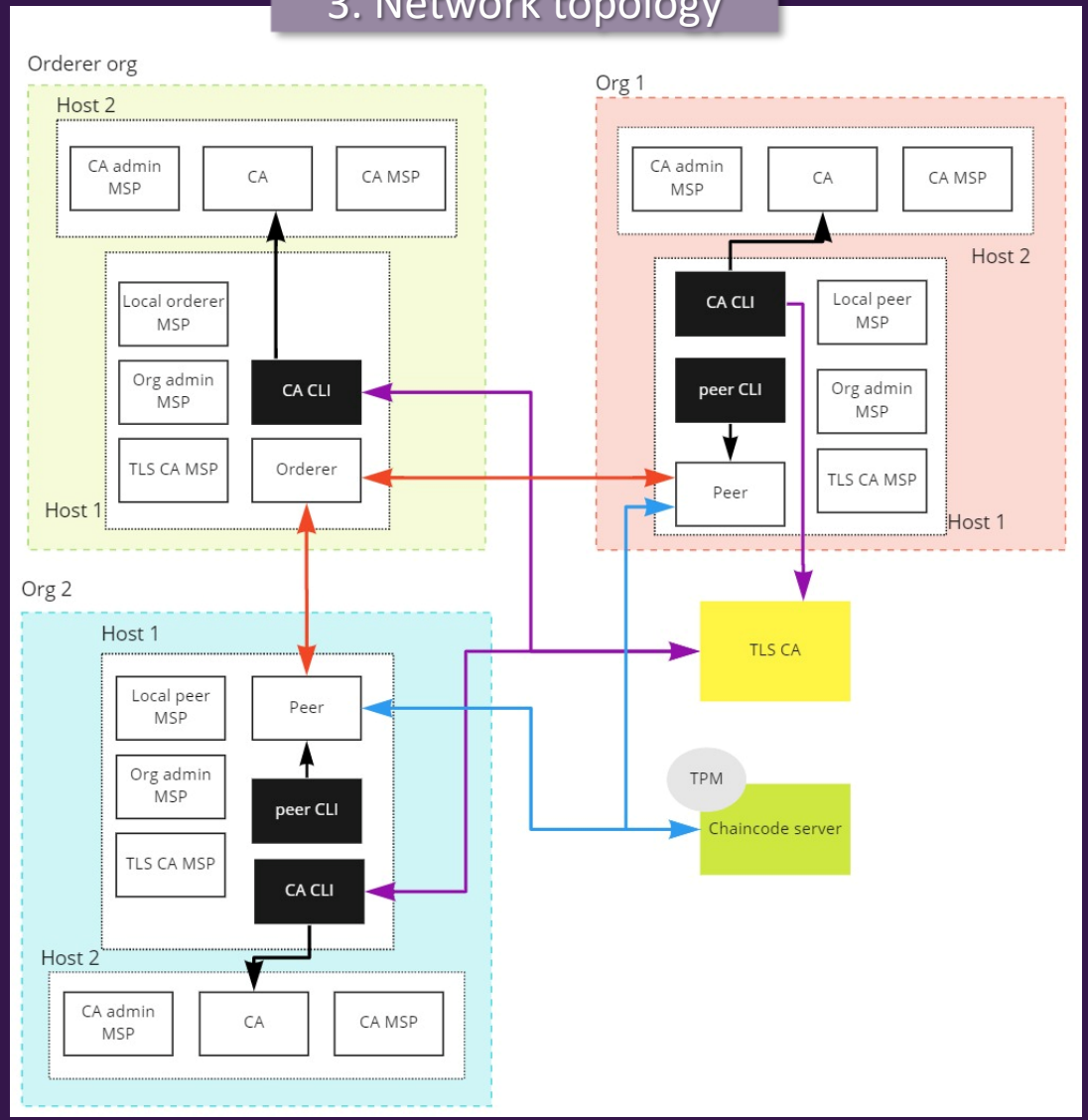
1. Research question

How to sign Hyperledger fabric smart contract using the TPM?

2. Methodology

- **Virtual machine**
  Hyper-v
- **Operating System**
  Ubuntu 20.04
- **Distributed ledger software**
  Hyperledger fabric
- **Development language**
  Go
- **TPM communication library**
  Go-TPM
- **Benchmark tool**
  Hyperledger Caliper

3. Network topology



4. Algorithm

Algorithm 1 SignAsset

$pubKey, privKey \leftarrow$ TPMGenKeyPair()
$hash \leftarrow$ sha256(asset)
$sig \leftarrow$ TPMSign(hash, privKey
storeOnChain(sig, pubKey, asset)

Algorithm 2 VerifyAsset

$sig, pubKey, asset \leftarrow queryLedger(assetID)$
$hash \leftarrow sha256(asset)$
if TPMVerify(hash, pubKey, sig) **then**
  return true
else
  return false
end if

5. Conclusion

It is possible, but I do not have performance data yet.

Full code available at: https://gitlab.com/HeyZedd/tpm-smart-contract