Laboratory_07: Signing docker images

This laboratory covers signing image process using cosign tool.

Install cosign tool

- curl -O -L "https://github.com/sigstore/cosign/releases/latest/download/cosign-linux-amd64"
- sudo mv cosign-linux-amd64 /usr/local/bin/cosign
- sudo chmod +x /usr/local/bin/cosign

Install docker tool

- Ubuntu | Docker Docs

Install docker tool

- Create a docker hub account

Generate signing keys

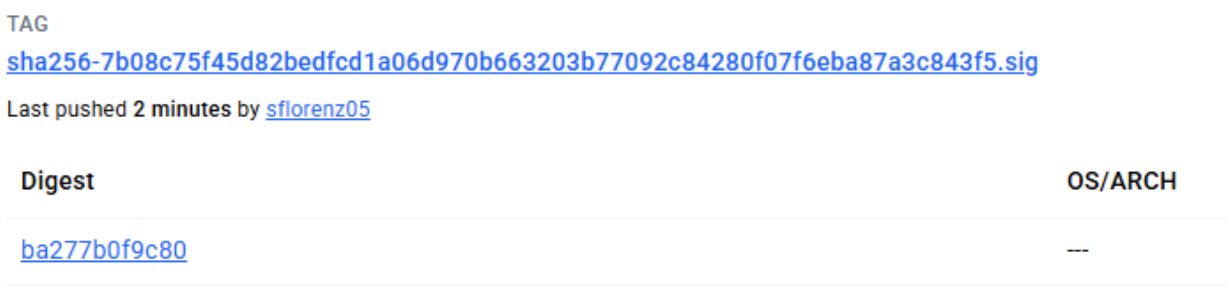
In this section, we'll create and use a public/private key pair for the signing and verification steps.

1. Create a public/private key pair for signing
    a. cosign generate-key-pair

Work with test docker image

2. Use docker pull command:
    a. docker pull lucj/btcprice:0.0.4
    b. docker pull lucj/btcprice:0.0.5
3. Copy image digest for both images:
    a. Digest: sha256:7b08c75f45d82bedfcd1a06d970b663203b77092c84280f07f6eba87a3c843f5

4. Tag the test image according to your dockerhub user:
    a. docker tag lucj/btcprice:0.0.4 sflorenz05/btcprice:0.0.4
    b. docker tag lucj/btcprice:0.0.5 sflorenz05/btcprice:0.0.5
5. Signing an image
    a. cosign sign --key cosign.key sflorenz05/btcprice@sha256:e14812c2d6d827a9402b8109c65e024fcd04cb4f998d59329e816a9c908a4e23
6. Review signed image:



7. Verify signed image:
    a. cosign verify --key cosign.pub sflorenz05/btcprice@sha256:7b08c75f45d82bedfcd1a06d970b663203b77092c84280f07f6eba87a3c843f5
8. Analyze the JWT obtained: JSON Web Tokens - jwt.io