Laborator work nr. 5

Theme: Public Key Infrastructure(PKI) and Digital Signature Algorithm (DSA)

Conditions:

Create an internal PKI using the OpenSSL tool. The generation of the root private key and the initialization of a Certified Authority (CA) are required. A self-signed certificate is created for the CA. System must be able to issue and revoke the private key for the user so that he can subsequently generate a digital signature. Each user/entity that obtains a signature will be able to sign the document/file and verify this signature. For the realization of this laboratory, the use of any language is allowed, including script languages such as Bash, PowerShell, zsh etc.

Requirements:

- Use algorithm RSA for generating private keys.
- Users' private keys validity is 365 days and dimension keys are minimum 2048 bits.
- Private key dimension for CA is 4096 bits and expired time for self-signed certificate in 10 years (3650 days)

Example of implementation - https://medium.com/@yakuphanbilgic3/create-self-signed-certificates-and-keys-with-openssl-4064f9165ea3