Laboratory Work No. 5

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 Certificate Authority (CA) are required. A self-signed certificate must be created for the CA.

The system must be able to issue and revoke private keys for users so that they can subsequently generate a digital signature. Each user or entity that obtains a signature must be able to sign a document or file and verify this signature.

For the realization of this laboratory, the use of any programming language is allowed, including scripting languages such as **Bash**, **PowerShell**, or **zsh**.

Requirements

- Use the **RSA** algorithm for generating private keys.
- Users' private keys must have a validity period of **365 days**, and their key length must be at least **2048 bits**.
- The private key of the Certificate Authority (CA) must be **4096 bits** long, and the expiration period for its self-signed certificate must be **10 years (3650 days)**.

Example of Implementation

A detailed example of creating self-signed certificates and keys with OpenSSL can be found at:

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