**Lucrarea de laborator #1**

Crearea infrastructurii de semnătură electronică

**Scopul lucrării:** Familiarizarea cu infrastructura națională de cheie publică.

Lucrarea de laborator constă în crearea unui model de infrastructură de cheie publică, similar celui național, utilizând instrumentul OpenSSL. Mai întâi se va crea autoritatea de certificare de nivel superior (eng. rootcertificationauthority, Root CA). Apoi se va crea autoritatea de certificare intermediară (eng. intermediate CA, sub-root CA). Certificatul cheii publice al autorității de certificare intermediară va fi semnat de către autoritatea de certificare de nivel superior. În final se vor crea certificate individuale pentru fiecare student. Certificatele individuale vor fi semnate de către autoritatea de certificare intermediară, astfel stabilindu-se un lanț de încredere persoana – autoritate de certificare intermediară – autoritate de certificare de nivel superior.

**Indicații de laborator**

1. Crearea autorității de certificare de nivel superior **root-ca**.
	1. Pe partiția logică destinată datelor (de regulă partiția D:) al calculatorului creați mapa **OpenSSL**.
	2. Accesați adresa internet <https://sourceforge.net/projects/openssl/?source=directory> pentru a descărca aplicația OpenSSL. Descărcați aplicația conform versiunii sistemului de operare în mapa creată.
	3. De la profesor copiați următoarele fișiere de configurare a aplicației OpenSSL:

**root-ca.conf**

**signing-ca.conf**

**dsig.conf**

Plasați aceste fișiere de configurare în mapa OpenSSL creată.

* 1. În mapa OpenSSL creați următoarea structură de mape pentru autoritatea de certificare de nivel superior:

**ca/root-ca**

**ca/root-ca/certs**

**ca/root-ca/crl**

**ca/root-ca/db**

**ca/root-ca/private**

* 1. Creați fișierele necesare bazei de date de certificate pentru a autoritatea de certificare.
		1. În mapa **ca/root-ca/db** creați fișierul **root-ca.db**. Inițial fișierul **root-ca.db** nu conține informație. Ulterior în acest fișier se vor înscrie datele despre certificatele emise de către autoritatea de certificare.
		2. În mapa **ca/root-ca/db** creați fișierul **root-ca.db.attr**. Acest fișier conține atribute de generare a certificatelor. Inserați în acest fișier următorul conținut și salvați fișierul:

**unique\_subject = no**

* + 1. În mapa **ca/root-ca/db** creați fișierul **root-ca.crl.srl**. Acest fișier conține contorul certificatelor revocate de către autoritatea de certificare. Inserați în acest fișier următorul conținut și salvați fișierul:

**01**

* + 1. În mapa **ca/root-ca/db** creați fișierul **root-ca.crt.srl**. Acest fișier conține contorul certificatelor emise de către autoritatea de certificare. Inserați în acest fișier următorul conținut și salvați fișierul:

**01**

* 1. Creați perechea de chei și cererea de semnare a certificatului cheii publice pentru autoritatea de certificare de nivel superior cu următoarea instrucțiune:

openssl req -new -config root-ca.conf -out ca/root-ca.csr -keyout ca/root-ca/private/root-ca.key

După procesul de generare a cheilor se va solicita setarea parolei pentru protejarea cheii private. Pentru moment utilizați parola **p@sswordca**.

În rezultat în mapa **ca/root-ca/private** va fi creat fișierul **root-ca.key**, care conține perechea de chei. Întrucât acest fișier conține cheia private el trebuie păstrat în siguranță.

În același timp în mapa **ca** a fost creată cererea de semnare a certificatului cheii publice – fișierul **root-ca.csr**.

* 1. Semnați certificatul cheii publice cu cheia privată generată la pasul precedent. Acest proces, când pentru semnarea certificatului cheii publice se utilizează cheia privată din aceeași pereche de chei se numește *auto semnare* (eng. self-signing). Atrageți atenția la parametrul –selfsign.

openssl ca -selfsign -config root-ca.conf -in ca/root-ca.csr -out ca/root-ca.crt -extensions root\_ca\_ext

La semnare se va cere să introduceți parola de acces la cheia privată.

Ca rezultat se va crea certificatul cheii publice (fișierul cu extensia **.crt**) pentru autoritatea de certificare de nivel superior **root-ca**. Spre deosebire de fișierul cu cheia privată **.key**, certificatul cheii publice poate fi distribuit publicului.

* 1. Importați certificatul cheii publice al autorității de certificare în repozitoriul de certificate al sistemului de operare (certificate store).
		1. Acționați dublu click pe fișierul root-ca.crt. Va apărea un dialog, care prezintă detaliile certificatului.



Atrageți atenția la mesajul din panoul Certificate Information, care ne spune că certificatul nu este unul de încredere.

Accesați pagina Details pentru a vedea detaliile certificatului.



Reveniți la pagina General a dialogului și apăsați butonul Install Certificate pentru al înscrie ca certificat de încredere.

* + 1. În dialogul ce apare Certificate Import Wizard selectați CurrentUser și apăsați Next.



* + 1. La pasul următor selectați opțiunea Place all certificates in the following store și apăsați butoul Browse pentru a selecta repositoriul de certificate în care se va instala certificatul pentru root-ca.



Din dialogul Select Certificate Store alegeți repozitoriul TrustedRootCertificationAuthorities și apăsați OK.



Apăsați Next, apoi în dialogul de confirmare iarăși apăsați Finish.

În dialogul de avertizare apăsați Yes



În rezultat se va afișa confirmarea importării certificatului.



Apăsați OK pentru a închide fereastra de confirmare.

Închideți dialogul Certificate.

* + 1. Acționați din nou dublu click pe fișierul root-ca.crt. Din nou apare dialogul Certificate, însă de această dată certificatul este de încredere și nu apare mesaj de alertă.



Autoritatea de certificare de nivel superior este funcțională.

1. Crearea autorității de certificare intermediare.
	1. În mapa OpenSSL creați următoarea structură de mape pentru autoritatea de certificare intermediară **signing-ca**:

**ca/signing-ca**

**ca/signing-ca/certs**

**ca/signing-ca/crl**

**ca/signing-ca/db**

**ca/signing-ca/private**

* 1. Creați fișierele necesare bazei de date de certificate pentru autoritatea de certificare.
		1. În mapa **ca/signing-ca/db** creați fișierul **signing-ca.db**. Inițial fișierul **signing-ca.db** nu conține informație. Ulterior în acest fișier se vor înscrie datele despre certificatele emise de către autoritatea de certificare.
		2. În mapa **ca/signing-ca/db** creați fișierul **signing-ca.db.attr**. Acest fișier conține atribute de generare a certificatelor. Inserați în acest fișier următorul conținut și salvați fișierul:

**unique\_subject = no**

* + 1. În mapa **ca/signing-ca/db** creați fișierul **signing-ca.crl.srl**. Acest fișier conține contorul certificatelor revocate de către autoritatea de certificare. Inserați în acest fișier următorul conținut și salvați fișierul:

**01**

* + 1. În mapa **ca/signing-ca/db** creați fișierul **signing-ca.crt.srl**. Acest fișier conține contorul certificatelor emise de către autoritatea de certificare. Inserați în acest fișier următorul conținut și salvați fișierul:

**02**

* 1. Creați perechea de chei și cererea de semnare a certificatului cheii publice pentru autoritatea de certificare intermediară cu următoarea instrucțiune:

openssl req -new -config signing-ca.conf -out ca/signing-ca.csr -keyout ca/signing-ca/private/signing-ca.key

După procesul de generare a cheilor se va solicita setarea parolei pentru protejarea cheii private. Pentru moment utilizați parola **p@sswordcas**.

În rezultat în mapa **ca/signing-ca/private** va fi creat fișierul **signing-ca.key**, care conține perechea de chei. Întrucât acest fișier conține cheia private el trebuie păstrat în siguranță.

În același timp în mapa **ca** a fost creată cererea de semnare a certificatului cheii publice – fișierul **signing-ca.csr**.

* 1. Semnați certificatul cheii publice a autorității de certificare intermediare cu cheia privată a autorității de certificare de nivel superior. De această dată nu se mai utilizează auto semnarea.

openssl ca -config root-ca.conf -in ca/signing-ca.csr -out ca/signing-ca.crt -extensions signing\_ca\_ext

La semnare se va cere să introduceți parola de acces la cheia privată a autorității de nivel superior.

Ca rezultat se va crea certificatul cheii publice pentru autoritatea de certificare intermediară **signing-ca**.

* 1. Importați certificatul cheii publice al autorității de certificare în repozitoriul de certificate al sistemului de operare (certificate store).
		1. Acționați dublu click pe fișierul root-ca.crt. Va apărea un dialog, care prezintă detaliile certificatului.



Atrageți atenția la mesajul din panoul Certificate Information, care ne spune că certificatul nu este unul de încredere.

Accesați pagina Details pentru a vedea detaliile certificatului.



Reveniți la pagina General a dialogului și apăsați butonul Install Certificate pentru al înscrie ca certificat de încredere.

* + 1. În dialogul ce apare Certificate Import Wizard selectați CurrentUser și apăsați Next.



* + 1. La pasul următor selectați opțiunea Place all certificates in the following store și apăsați butonul Browse pentru a selecta repositoriul de certificate în care se va instala certificatul pentru root-ca.



Din dialogul Select Certificate Store alegeți repozitoriul IntermediateCertificationAuthorities și apăsați OK.



Apăsați Next, apoi în dialogul de confirmare iarăși apăsați Finish.

În dialogul de avertizare apăsați Yes



În rezultat se va afișa confirmarea importării certificatului.



Apăsați OK pentru a închide fereastra de confirmare.

Închideți dialogul Certificate.

* + 1. Acționați din nou dublu click pe fișierul **signing-ca.crt**. Din nou apare dialogul Certificate, însă de această dată certificatul este de încredere și nu apare mesaj de alertă.



Autoritatea de certificare intermediară este funcțională.

1. Emiterea certificatului cheii publice pentru o persoană
	1. În mapa **OpenSSL** creați mapa **certs** pentru stocarea certificatelor individuale.
	2. Generați perechea de chei și cererea de certificare cu următoarea instrucțiune

openssl req -new -configdsig.conf -out certs/**[student]**.csr -keyout certs/**[student]**.key

În locul textului **[student]**fiecare student își va indica inițialul prenumelui și numele de familie. Ex. Ion Cojocaru – **icojocaru**.

La generare se va cere setarea unei parole pentru protejarea cheii private.

În mapa **certs** au apărut fișierele cu extensia .**csr** (certificate signingrequest) și .**key** (perechile de chei).

* 1. Cererea de semnare a certificatului cheii publice se transmite autorității de certificare intermediare pentru semnare. Autoritatea de certificare intermediară semnează certificatul cheii publice al persoanei.

openssl ca -config signing-ca.conf -in certs/**[student]**.csr -out certs/**[student]**.crt -extensions qualified\_ext

Fișierul .**crt** emis reprezintă certificatul cheii publice a persoanei, semnat de autoritatea de certificare intermediară și se transmite solicitantului.

* 1. Apăsați dublu click pe fișierul **[student].crt**

În dialogul Cerificate observați detaliile certificatului.

Pe pagina CertificationPath a dialogului observați lanțul de încredere creat între persoana, autoritatea de certificare intermediară și autoritatea de certificare de nivel superior.



1. Pregătiți nota explicativă a lucrării cu concluziile și constatările de rigoare. Ulterior aceasta va fi transmisă profesorului semnată electronic cu cheia privată a studentului, conform instrucțiunilor lucrării de laborator nr. 2.

RESURSE:

1. <https://www.openssl.org/>
2. <https://www.sslshopper.com/article-most-common-openssl-commands.html>
3. <http://www.oid-info.com/cgi-bin/display?oid=1.2.498.3&action=display>