Aplicatie web,
Tehnologie web: ASP.NET CORE.

Tema Proiect: Generator de certificate criptografice pentru semnarea documentelor

Aplicatia mea este folosita in contextul in care ai nevoie sa semnezi(criptografic) un document sau sa verifici daca documentul este semnat de o anumita persoana(utilizator in cazul nostru). Pentru asta se va folosi o criptare asymetrica, unde este nevoie de o cheie privata si una publica.

Din perpectiva unui utilizator, acesta poate sa isi genereze un certificat(care contine cheia publica) si cheia privata, cu aceasta(cheia privata) el are posibilitatea de a isi semna documentul dorit, cheia publica va fi stocata pe serverul aplicatiei, acest utilizator trebuie sa retina mereu cheia privata. In momentul in care utilizatorul semneaza un document, trebuie sa introduca cheia privata, documentul si i se va returna un fisier cu functia hash a documentului criptata. Cand utilizatorul doreste sa verifice daca un anume document a fost semnat de un anume utilizator, trebuie sa introduca numele, sa incarce documentul si fisierul cu functia hash criptata(de utilizatorul care a semnat criprografic documentul). Iar aplicatia mea trebuie sa decripteze functia hash cu acea cheie publica si sa faca hash asupra documentului ca dupa aceasta sa compare acele doua hash-uri, in cazul in care acestea sunt la fel, inseamna ca documentul a fost semnat de catre acel utilizator.

Niste detalii finale, dupa ce o sa fac aceasta aplicatie functionabila vreau sa fac autentificarea pe roluri, un utilizator sa poata sa isi genereze un certificat odata pe luna, pe an, sau oricand.

Aceasta aplicatie vreau sa o dezvolt in ASP.NET CORE, eu am inceput implementarea ei recent(3 saptamani in urma), tehnologia aceasta este noua pentru mine, intalnesc concepte noi si dificultati pe care le rezolv in cele din urma, insa imi ia mai mult timp.

Ce am facut pana acum la aplicatie:

Am facut partea de autentificare folosind nume de utilizator si parola, validarea la inregistrarea utilizatorului. La nivel de aplicatie am generat un certificat si o cheie privata.
In prezent lucrez la partea de generare a certificatului(si cheii) si semnare a documentului de catre utilizator.

Imi doresc ca in final aplicatia mea sa fi sigura de folosit si functionala.