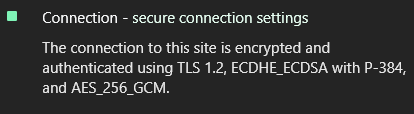
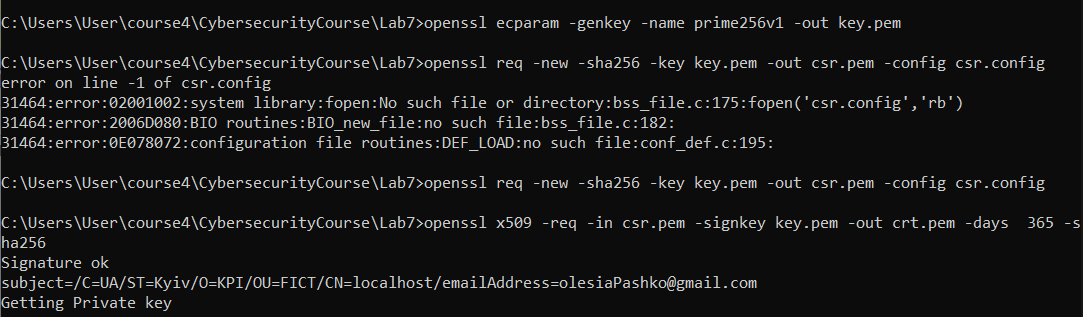
Для лабораторної роботи використовувалась остання версія протоколу TLS - TLSv1.2 як видно із скріна інструментів розробника Chrome нижче. Я обрала останню версію оскільки вона є найбільш безпечною.

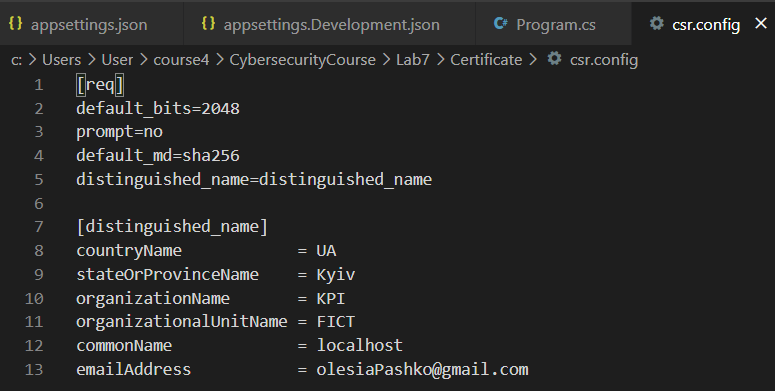
Як набір алгоритмів для безпечного передавання даних був використаний ECDHE\_ECDSA with P-384, and AES\_256\_GCM. ECDHE\_ECDSA означає Elliptic Curve Diffie-Hellman та Elliptic Curve Digital Signature Algorithm для погодження ключів протягом TLS рукостискання. AES\_256\_GCM означає, що саме цей алгоритм використовується для подальшого обміну даними. Цей ciphersuite на даний момент вважається доволі безпечним тому я обрала саме його.



Для генерації сертифікату був використаний openssl, як показано на рисунку нижче



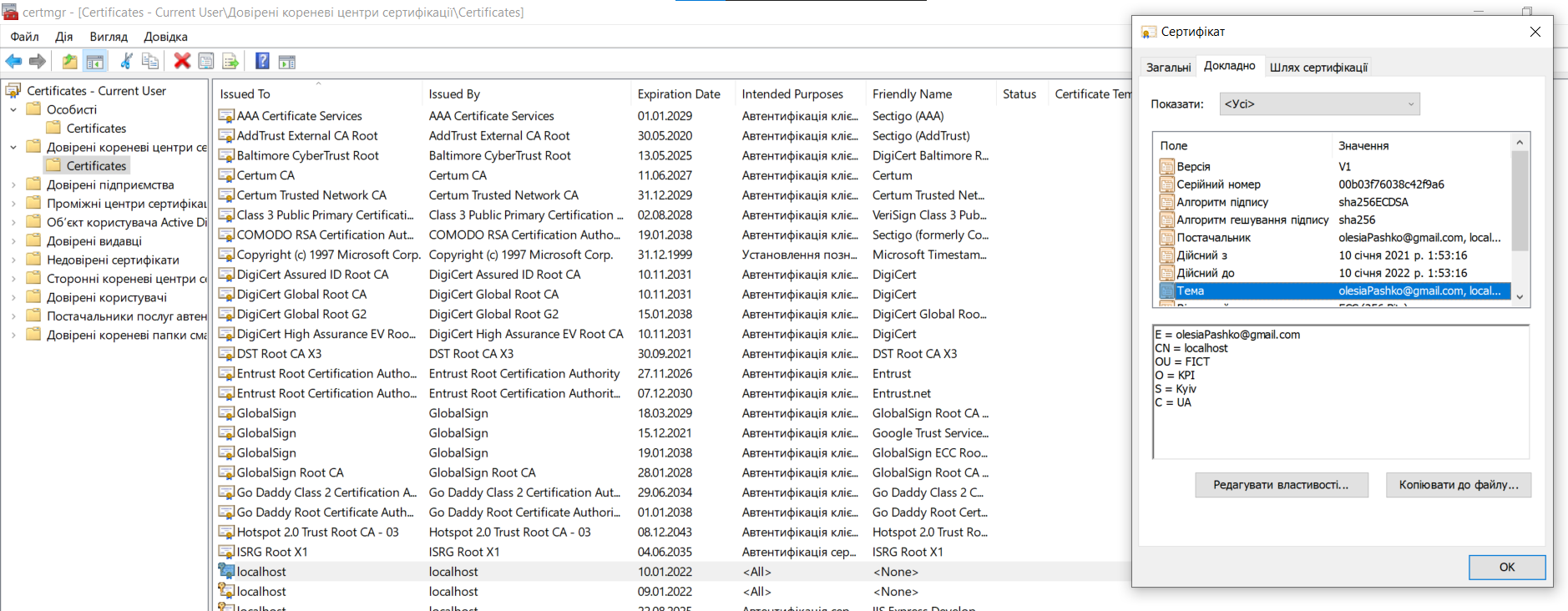
Як файл конфігурацій використовувався наступний файл



Далі, щоб додати даний сертифікат в застосунок на ASP.NET слід згенерувати на основі приватного ключа та сертифіката .pfx файл. Відповідна команда наведена нижче



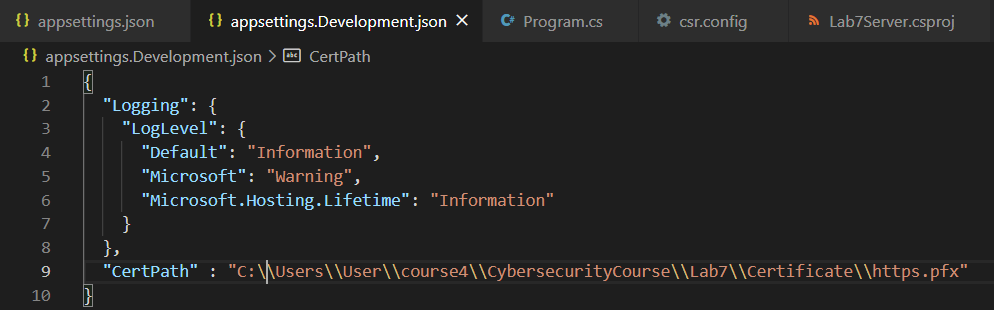
Даний .pfx файл слід помістити до довірених сертифікатів операційної системи. Це можна зробити з допомогою утиліти Windows certmgr



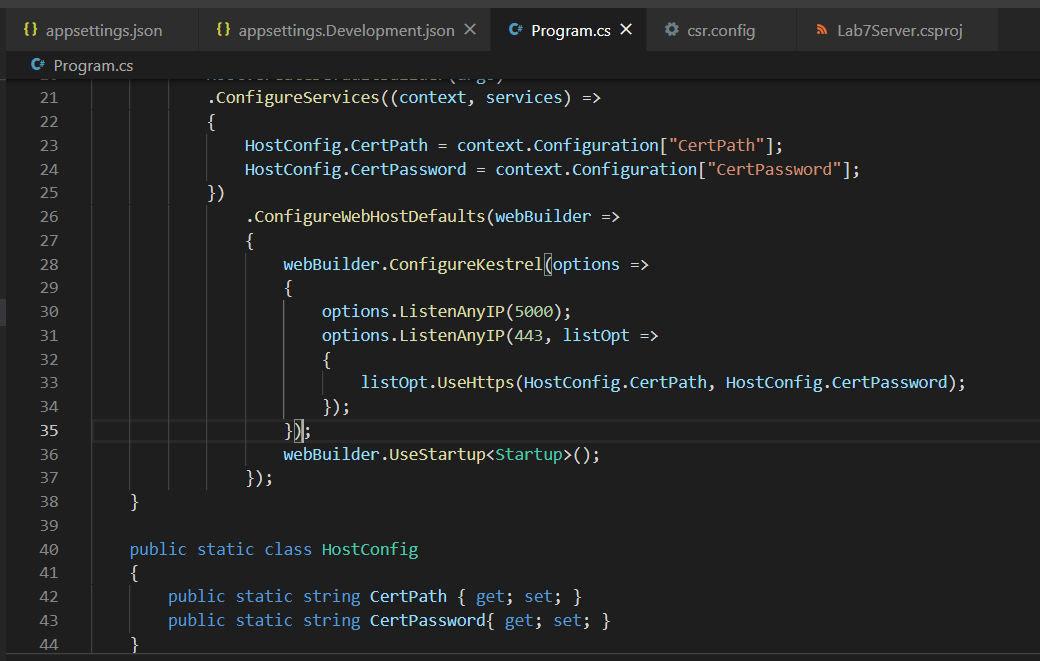
Для збереження паролю, який серверу необхідно вказувати при використанні .pfx файлу було використане сховище секретів .net. Відповідна команда наведена нижче



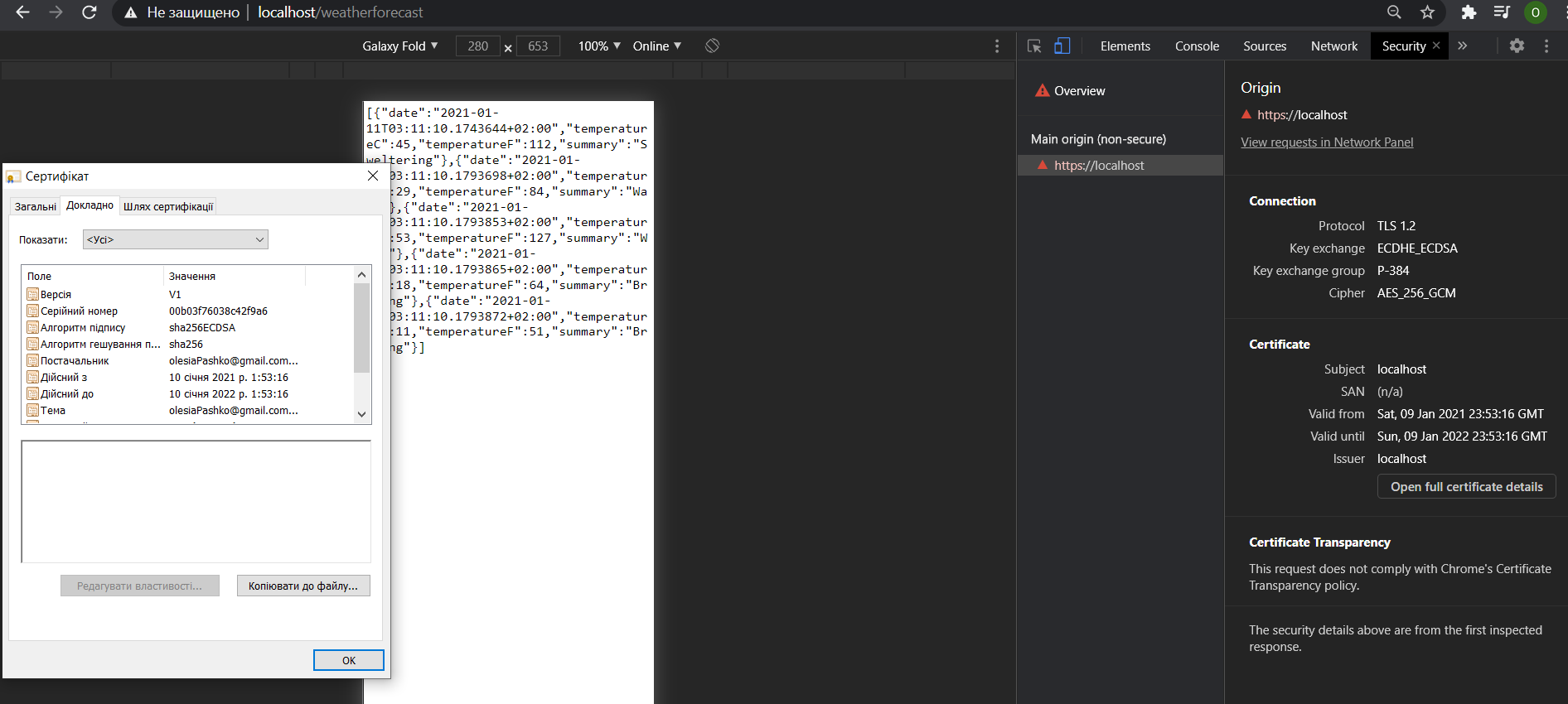
Шлях до сертифікату був записаний в appsetting.Development.json



Нижче наведено код, який витягає шлях до сертифікату та пароль з конфігурацій та запускає сервер



Сертифікат та запущений сервер можна побачити нижче



Chrome вважає зв’язок ненадійним оскільки ми видали даний сертифікат собі самі, а не попросили його підписати якимось Intermediate certificate.

Сертифікат можна зберігати поряд із кодом застосунку оскільки це є публічною інформацією, але приватний ключ нам слід зберігати деінде. Хорошим варіантом є використання Azure або AWS або GCP служби для збереження ключів в продакшині та місця на локальній машині із обмеженими правами доступу для development режиму, для MAC OS хорошим варіантом є KeyChain. Хоча .pfx файл і захищений паролем, але, оскільки він містить приватний ключ всердині, його все одно слід поміщати в місця з обмеженими правами доступу на рівні операційної системи.