MotivSMA: Certificate Generation for HTTPS browsing

Necessary for the connection between sma-client (frontend) and sma-server (backend)

Carmen Areses Sánchez, Pilar Bourg, Pablo Hervalejo, Carlota Laverón, Alejandra O'Shea

Table of contents:

1. Introduction

1.1. General aspects

HTTPS encrypts all data and requests travelling on the network automatically, ensuring confidentiality and preventing data leaks.

A certificate allows the browser to verify who the server is and that the connection is not being intercepted. Without the certificate, the browser would not trust the server; meaning that a certificate is necessary to run MotivSMA.

MotivSMA uses SpringBoot, which in turn uses TLS to support HTTPS. To enable TLS it needs:

- A **private key**
- A **public certificate**
- Bundled together inside a **keystore file (PKCS#12 .p12)**

1.2. Prerequisites

- Chocolatey allows for a simple mkcert installation in Windows
- Mkcert generates an SSL sertificate (P12 file) necessary for SpringBoot to activate the HTTPS network connection.

2. Certificate generation and configuration on sma-server (backend)

If the certificate found in GitHub is not providing the expected outcomes and the connection between sma-server and sma-client is not successful, it is recommended to create a new certificate following the steps given in this section:

2.1. Creation of the certificate

On the terminal of the sma-server project write:

```
mkcert -pkcs12 telemedicine.p12 localhost 127.0.0.1 telemedicine
```

- A P12 file with name "*telemedicine.p12*" must have been created in the root of the project.
- The automatic password for certificates generated this way is: *changeit*

You must know the alias your P12 file is under, for that write in the same terminal:

```
keytool -list -v -keystore telemedicine.p12+3.p12 -storepass changeit
```

A lot of information will appear on the terminal, but you must look for the alias:

2.2. Configuration in *sma-server*

Now, you must relocate "telemedicine.p12" from the root to *src/main/resources*. Once this has been done successfully and you need to know:

- The alias
- The password
- Where it has been stored (! Must be in *src/main/resources*)

Moreover, you must configure your application-local.yml (! Must be in *src/main/resources*). Add:

```
server:
  port: 8443
  ssl:
    enabled: true
    key-store: src/main/resources/{FILE_NAME}.p12
    key-store-password: {PASSWORD}
    key-store-type: PKCS12
    key-alias: {YOUR_ALIAS}
```

Highlights must correspond to your admin parameters; these will be used to log into the system

2.3. Final steps

Finally, you must do:

```
mvn clean package
```

```
mvn spring-boot:run
```

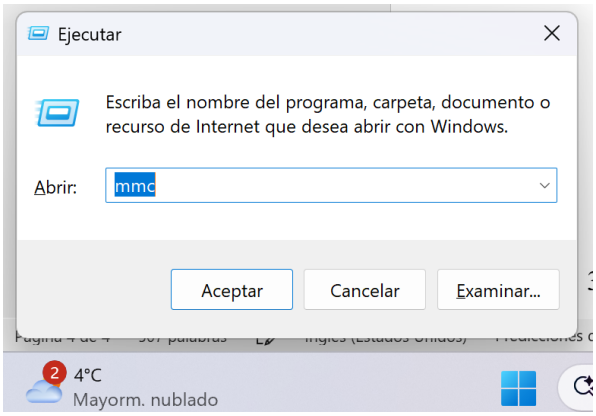
3. If problems persist

If after generating the key, the connection between the front-end and back-end of the website is not successfully established, there are two possible solutions you must follow.

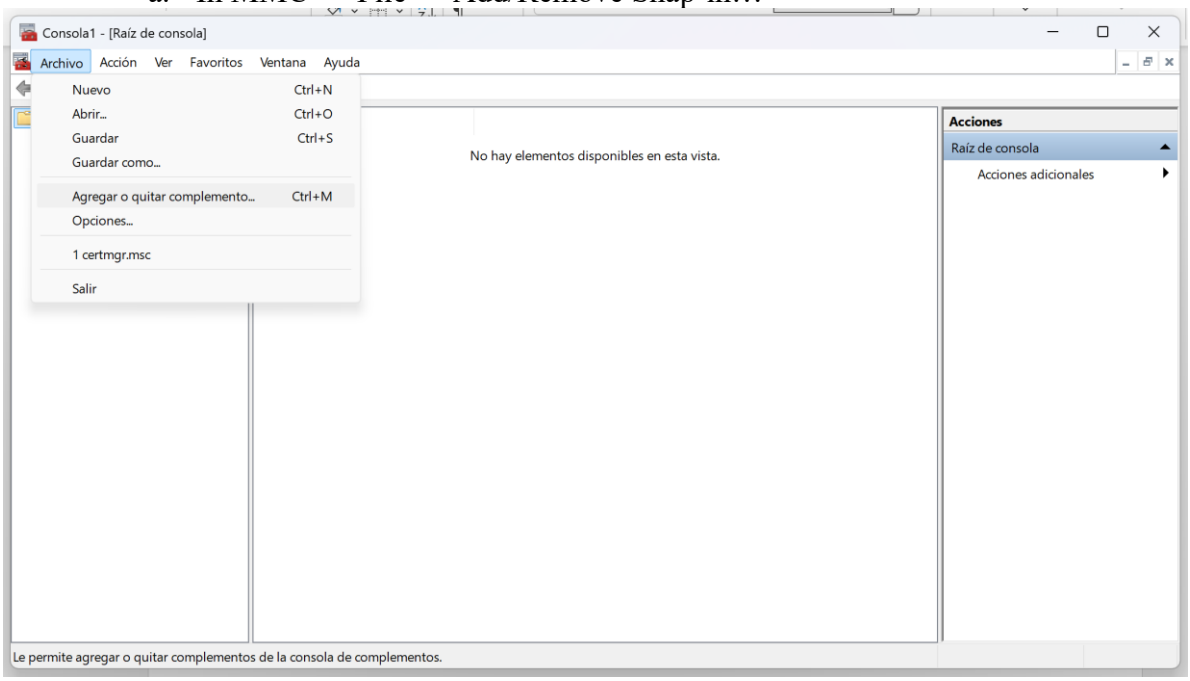
3.1. Integration of certificate in the computer

First, install the CRT certificate on your computer:

1. Open Microsoft Management Console (Win+R)



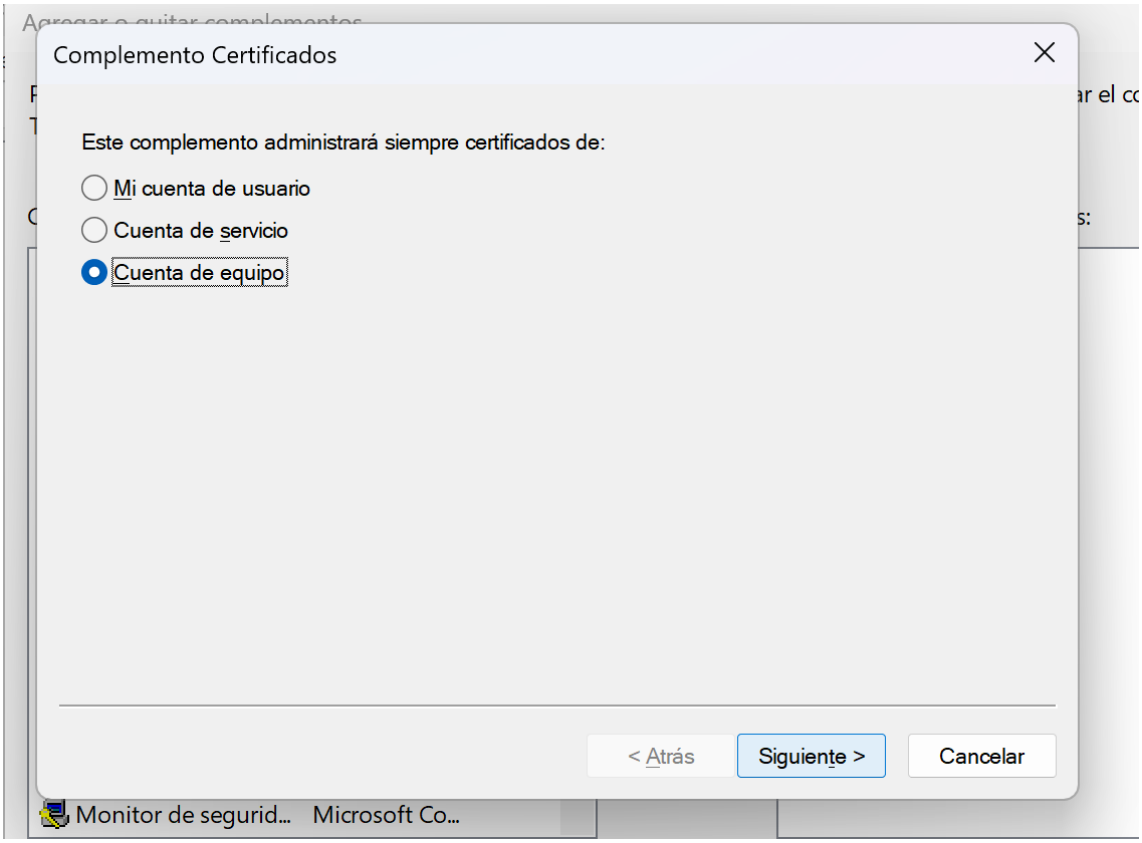
2. Add the Certificates snap-in
    a. In MMC → File → Add/Remove Snap-in…



    b. Select Certificates

    c. Click Add

    d. Choose Computer account



e. Click Next → Finish

f. Click OK

3. Import the Root CA

a. Expand Certificates (Local Computer)

b. Expand “Trusted Root Certification Authorities”

c. Right-click Certificates → All Tasks → Import

d. Click Next

e. Browse to where your certificate is located

f. Select it → Open

g. Continue → Place in: Trusted Root Certification Authorities

h. Click Finish

3.2. Integration of certificate in browser

Furthermore, the browser must trust the network communication system (HTTPS) as well, allowing endpoints to communicate successfully between frontend and backend. For this, follow these steps:

1. Go to configuration in your Chrome browser
2. In settings go to: Settings → Privacy and Security → Security
3. At the end of this section click on “Manage certificates” it should open a new tab in the browser
4. Go to “Local certificates” → Installed by you
5. Trusted Root Certification Authorities → Import → Select the CRT certificate and accept all prompts