2.1 - Tecnologías de Servicios de Internet

Tema 9b - https

Universidad Rey Juan Carlos

Nicolás Rodríguez
nicolas.rodriguez@urjc.es

code URJC

https

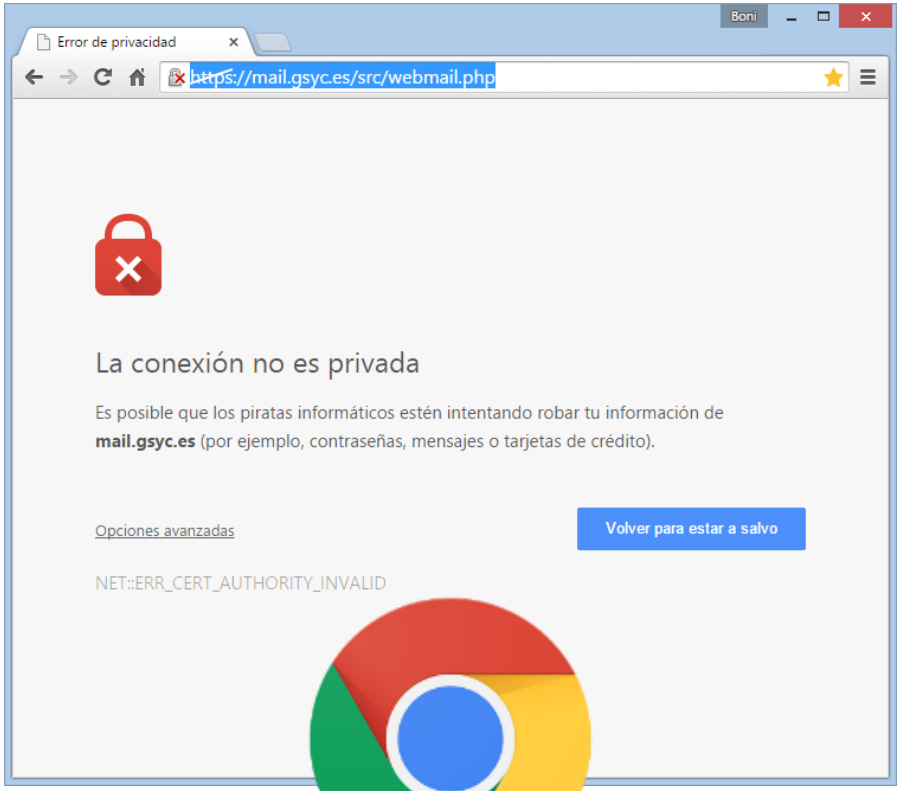
- **HTTPS** *(Hypertext Transfer Protocol Secure)*: Versión segura de HTTP
- Con https se consigue que toda la información que se intercambie un **navegador** web con un **servidor** web esté **cifrada**
- Es decir, un usuario malicioso no podrá entender la información que viaja por la red
- https utiliza criptografía de **clave pública** y se apoya en el estándar **TLS**

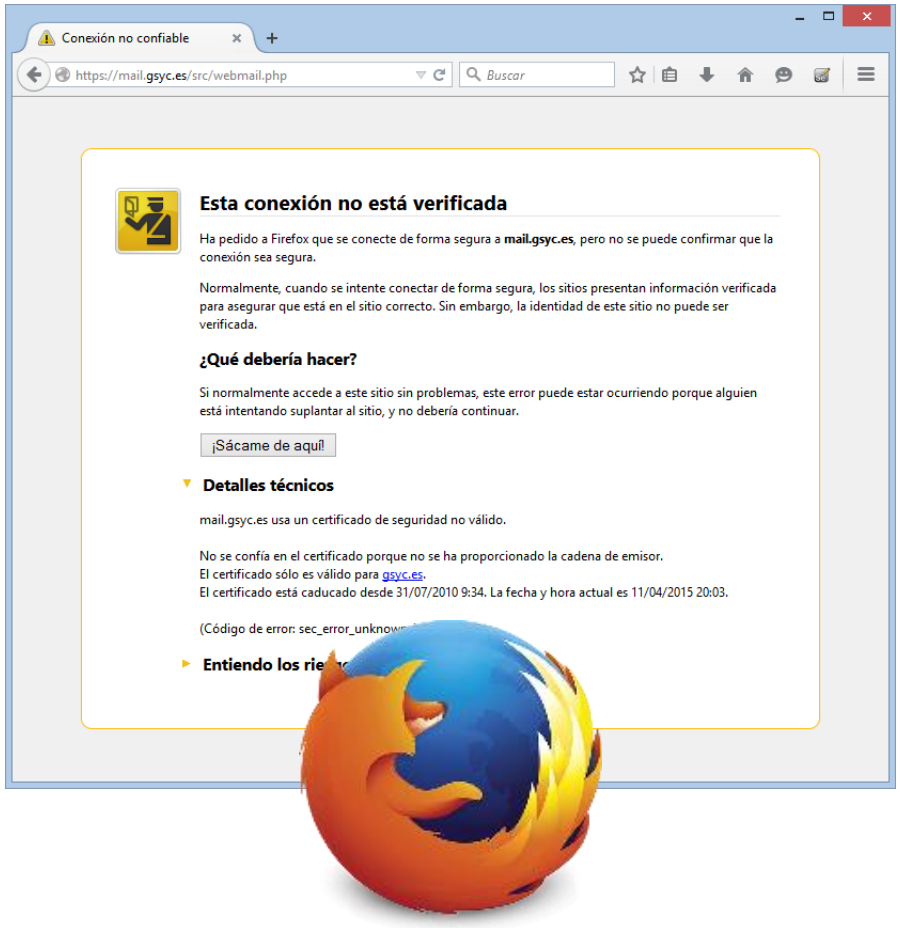
https

- Los navegadores tienen una **lista de CA** en la que confían
- Si se conectan a un servidor web y presenta un certificado que esté firmado por una CA no reconocida, se muestra un **aviso al usuario**.

https

code URJC





https

- Un certificado está asociado a un dominio y se puede conseguir de dos formas diferentes:
  - **Comprándolo a una CA:**
    - Puede costar entre **10€ y 1000€** anuales.
    - Existen muchas empresas dedicadas a este negocio
  - **Obteniéndolo de Let's Encrypt:**
    - Entidad sin ánimo de lucro que proporciona certificados de confianza (Let's Encrypt es una CA). Apoyada por Facebook, Mozilla, ...
    - Hasta 20 certificados a la semana, 3 meses de validez
    - Herramientas para obtención y renovación automática
  - **Creándolo uno mismo:**
    - Es gratis
    - Los navegadores mostrarán el **aviso** de entidad no reconocida a los usuarios

https

- **Comunicación cifrada con https**
  - Usando un **certificado autofirmado** podríamos sufrir un ataque y nuestros datos podrían ser descifrados
  - Si usamos un **certificado de una CA,** nuestros datos no podrán ser descifrados ni alterados

https

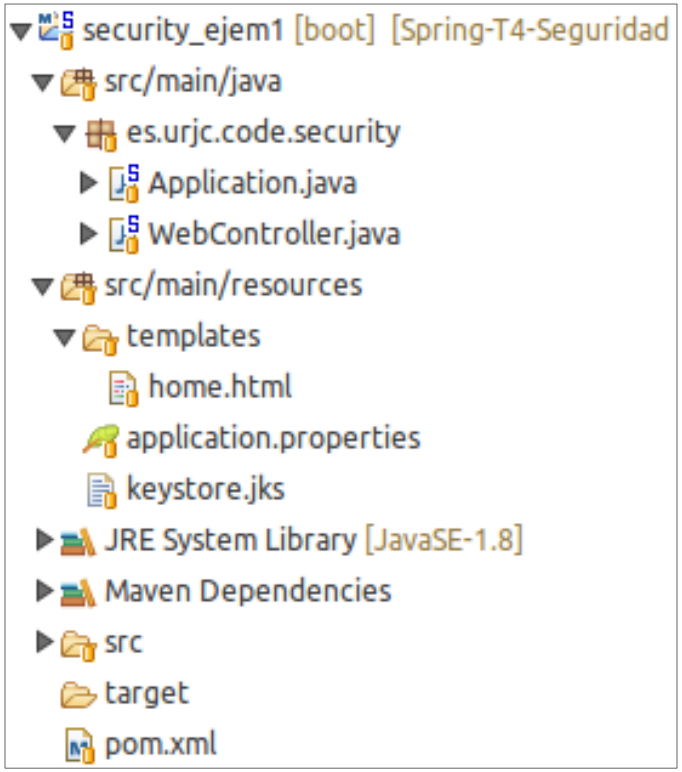
- Iniciamos CMD como administrador, y ejecutamos:
- cd C:\Program Files\Java\jdk-11.0.5\bin

- Una vez aquí, ejecutamos lo siguiente:
- keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass password -validity 360 -keysize 2048

- ¿Cuáles son su nombre y su apellido?
- [Unknown]: X Y
- ¿Cuál es el nombre de su unidad de organización?
- [Unknown]: Computer Science and Statistics Department
- ¿Cuál es el nombre de su organización?
- [Unknown]: URJC
- ¿Cuál es el nombre de su ciudad o localidad?
- [Unknown]: Madrid
- ¿Cuál es el nombre de su estado o provincia?
- [Unknown]: Madrid
- ¿Cuál es el código de país de dos letras de la unidad?
- [Unknown]: ES
- ¿Es correcto CN=X Y, OU=Computer Science and Statistics Department, O=URJC, L=Madrid, ST=Madrid, C=ES?
- [no]: si

https

Creamos un ejemplo sencillo, por ejemplo, el "Hello World"

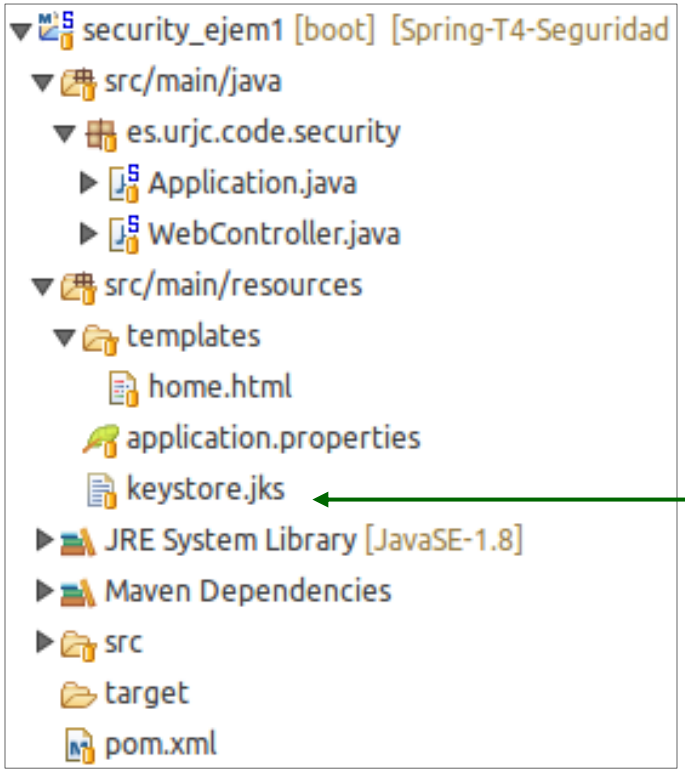


pom.xml

```
<dependencies>
 <dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-web</artifactId>
 </dependency>
 <dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-mustache</artifactId>
 </dependency>
</dependencies>
```

https

Creamos un ejemplo sencillo, por ejemplo, el "Hello World"



application.properties

```
server.port = 8443
server.ssl.key-store = classpath:keystore.jks
server.ssl.key-store-password = password
#server.ssl.key-password = secret
```

Fichero que contiene el certificado autofirmado generado con la herramienta del JDK **keytool**