

# **Anexo IV**

## **Manual del usuario**

### *Sistema de Prestación de Servicios de Certificación Electrónica*

**Trabajo de Fin de Grado**  
**Grado en Ingeniería Informática**



**VNiVERSiDAD**  
**DSALAMANCA**

Autor

Tomás Calderón López

Tutor/a

Ángel Luis Sánchez Lázaro

# Tabla de contenido

<i>Introducción</i> .....	<b>3</b>
<b>1. Registro, verificación e inicio de sesión</b> .....	<b>4</b>
<b>2. Certificados</b> .....	<b>7</b>
<b>3. Firmas</b> .....	<b>9</b>

# **Introducción**

El propósito principal de este Manual del Usuario es brindar una guía completa y accesible para que los usuarios puedan aprovechar al máximo el portal web. A lo largo de este documento, se realizará un examen detallado de las funcionalidades disponibles, proporcionando instrucciones claras y ejemplos prácticos que permitirán a los usuarios comprender, utilizar eficazmente la plataforma y comprender la información necesaria para interactuar de manera efectiva con el sistema.

Ofrece una visión detallada de las características y capacidades de la aplicación, lo que facilita la adopción rápida y el aprovechamiento completo de sus recursos. Además, este manual también puede servir como un recurso de referencia valioso para resolver preguntas comunes y abordar desafíos que los usuarios puedan encontrar en su uso cotidiano.

# 1. Registro, verificación e inicio de sesión

Nada mas entrar en la aplicación, el usuario será redirigido al índice:



TCert Inicio Iniciar Sesión Registro

## TCERT

En un mundo cada vez más digitalizado, la seguridad en línea es de gran importancia. Garantizar la protección de los datos y la privacidad de la información transmitida a través de la web es esencial en la era de la información. Una de las herramientas fundamentales en la protección de la comunicación en línea es la tecnología HTTPS (TLS) y el uso de certificados digitales. Esta página web ha sido creada con el propósito de mostrar un pequeño anticipo y facilitar la comprensión de la configuración segura, el uso de certificados y demás aspectos relacionados con la seguridad. Aquí, exploraremos desde los conceptos fundamentales hasta las implementaciones prácticas, con el objetivo de comprender los conocimientos necesarios para asegurar la comunicación en línea.

### Proceso de Configuración Segura de Servidores

En esta sección, se explicará la configuración segura de este servidor, que esta creado en la plataforma Spring Boot Security, que a su vez se sirve de la herramienta Keytool de Java, utilizada a lo largo del proyecto.

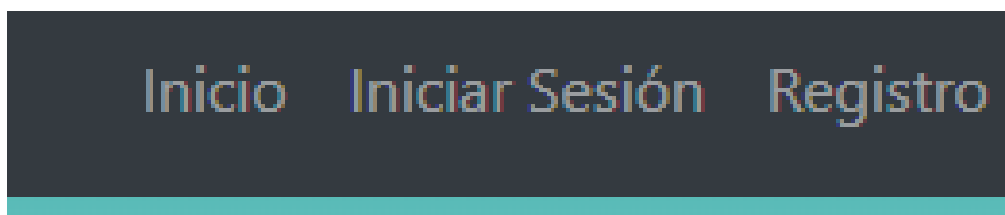
Cabe destacar que, aunque la explicación gire sobre este entorno en específico, la esencia del proceso es la misma para cualquier tecnología.



### Antes de empezar: Configuración Segura Web y HTTPS

La configuración segura web y HTTPS es esencial para proteger la información transmitida entre los usuarios y un sitio web. Aquí se presenta una introducción a estos conceptos clave:

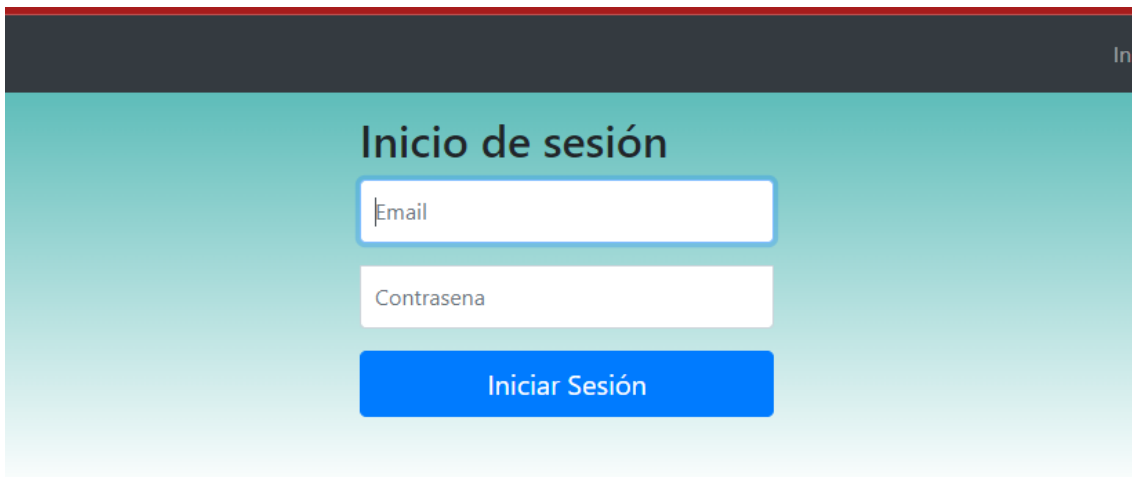
En esta pantalla de bienvenida se muestra información sobre lo que se va a encontrar en la página y sobre procesos de configuración. En la barra de navegación inicial se tienen tres opciones: Inicio, Iniciar Sesión y Registro. De momento Inicio redirigirá al inicio de sesión porque sirve para cuando el usuario se autentique con usuario, pueda ir a su página de inicio.





The registration form is titled "Registro" and is set against a teal background. It features three input fields: "Email", "Nombre", and "Contraseña". Below these fields is a blue button labeled "Registrarse".

El primer paso es registrarse, introduciendo las credenciales que el usuario estime, cuando lo haya hecho, se procesará la respuesta y será redirigido al inicio de sesión, donde ya podrá autenticarse con las credenciales con las que se registró.



The login form is titled "Inicio de sesión" and is set against a teal background. It features two input fields: "Email" and "Contraseña". Below these fields is a blue button labeled "Iniciar Sesión".

Una vez autenticado, se redirigirá al inicio de la aplicación, donde hay información sobre el cifrado pero lo importante es que se podrá ver un cambio en la navegación:

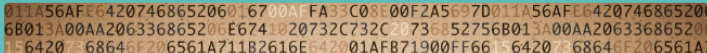
Inicio Certificados Firmas

## Bienvenido, Tomas

La pantalla principal se explica el proceso angular por el que se rigen todas las funcionalidades de la web: el **cifrado asimétrico**. Si quieres realizar estas actividades, por favor, usa la barra de navegación para desplazarte.

### Cifrado y Seguridad en Comunicaciones

La seguridad de las comunicaciones en línea es esencial en la era digital, y una parte fundamental de esta seguridad es el cifrado de datos. El cifrado es un proceso mediante el cual la información se convierte en un formato ilegible, a menos que se tenga la clave adecuada para descriptarla.



Inicio Certificados Firmas Cerrar Sesión

Al estar autenticado, se permiten ver las funciones de la página web, pero al intentar acceder a ellas se deniega el acceso, pues hay que verificar la cuenta antes:

## Acceso Denegado

Debes verificar tu correo electrónico antes de acceder a otros servicios. Por favor, comprueba tu email en busca de correo.

En el correo electrónico se habrá recibido un mensaje de esta índole:



tcert-no-reply@outlook.es

para mí ▼

## ¡Bienvenido, Tomas!

Por favor, verifique su cuenta:

<https://localhost:8088/verificar?c=1b76b7c9-2fbb-46e1-989a-4d4b222ac054>

¡Gracias!

Accediendo al enlace, el sistema verificará la cuenta, lo vuelve a redirigir al inicio y ahora las funciones sí están disponibles. Principalmente hay 2: Certificados y Firmas. Consultaremos primero la de certificados.

## 2. Certificados

**Certificados X.509**

Un certificado X.509 es un estándar utilizado en seguridad informática y criptografía para representar y verificar la autenticidad de entidades digitales, como sitios web y usuarios. Proporciona información sobre la entidad, incluyendo su clave pública, y está firmado por una Autoridad de Certificación de confianza. Los certificados X.509 se utilizan en HTTPS, correo electrónico seguro y autenticación en línea para garantizar la seguridad y la autenticación de las comunicaciones digitales.

Aquí es donde aparecerán los certificados que crees. El proceso se realiza completamente en el servidor:

- 1. Generación de Claves:** Se generan claves criptográficas: una clave privada (secreta) y una clave pública (compartida) con el algoritmo seleccionado.
- 2. Solicitud a la CA:** Se genera una solicitud a una Autoridad de Certificación (CA) para obtener un certificado digital. Esta solicitud incluye la clave pública y detalles de identificación del servidor.
- 3. Firma Digital:** El servidor utiliza su clave privada para firmar digitalmente la solicitud. El cliente puede verificar estas firmas utilizando el certificado emitido por la CA.
- 4. Descarga:** Una vez creado, se ensambla con la clave privada en formato .p12 para la disponibilidad completa de uso del usuario de su certificado generado.

[Crear Certificado](#)

Lista de certificados creados:

Esta página contiene información relacionada con los certificados, y abajo del todo aparecerán los certificados que cree el usuario. Al seleccionar “Crear Certificado” se redirige a la página con un formulario para personalizar el certificado, tanto los datos como el algoritmo (El CN debe ser el email, pues se utiliza para autenticarse).

**Crear Certificado X.509**

Todos los campos son opcionales

tomasc4@usa.les

Organización (O)

Unidad de Organización (OU)

Localidad (L)

Provincia (ST)

Código de País (C)

**Algoritmo a utilizar**

RSA con SHA-256

[Crear Certificado](#)

Una vez creado, se es redirijo a la página de certificados, donde aparece el certificado creado con los datos proporcionados y un enlace para descargar.

[Crear](#)

## Lista de certificados creados:

ID: n0

Datos: C=ES, ST=CA, L=Reinosa,  
OU=Facultad de Ciencias, O=USAL,  
CN=tomascl4@usal.es

Algoritmo: SHA256withRSA

[Descargar](#)

Se puede probar a descargar y utilizarlo para autenticarse. Al descargarlo simplemente se instala con doble click para almacenarlo en el almacén del sistema (o en el del navegador si se utiliza Firefox), no tiene contraseña, simplemente de forma automática se seleccionan las opciones preestablecidas. Una se instala, se presiona cerrar sesión. Si el navegador no detecta el certificado, hay que reiniciarlo para que cargue de nuevo el sistema y lo detecte. En el caso de Chrome, con poner **Chrome://restart** en la barra es suficiente, y al reiniciarse ahora sí aparecerá la opción de autenticado con certificado:

### Seleccionar un certificado

Selecciona un certificado para autenticar tu identidad en localhost:8088.

Asunto	Emisor	Número de serie
tomascl4@usal.es	TCertCA	018A702808EE

[Datos del certificado](#)

[Aceptar](#)

[Cancelar](#)

Tras seleccionar aceptar no se notará nada, pero si se presiona ahora inicio, será redirigido a la página de inicio del usuario, ya que ha sido autenticado.



### 3. Firmas

La otra funcionalidad del sistema son la creación y verificación de firmas.

## Firmas Digitales

Una firma digital es una técnica criptográfica utilizada para verificar la autenticidad e integridad de un mensaje o un documento digital. Se utiliza en una amplia variedad de aplicaciones, desde la seguridad de correos electrónicos hasta la autenticación de documentos legales.

Aquí es donde verás el proceso de crear y verificar firmas digitales:

[Crear/Verificar Firmas](#)

- Creación de Firma Digital:** Para crear una firma digital, primero generamos un resumen (hash) del contenido que queremos firmar. Luego, utilizamos nuestra clave privada para cifrar este resumen, lo que crea la firma digital.
- Verificación de Firma Digital:** Para verificar una firma digital, necesitamos el mensaje original, la firma digital y la clave pública equivalente a la clave privada introducida para firmar. Primero, generamos un resumen del mensaje original y luego utilizamos la clave pública para descifrar la firma digital y obtener otro resumen. Si los dos resúmenes coinciden, la firma es válida y el mensaje no ha sido alterado.

#### Firma

```
graph LR; Datos[Datos] -- Hash function --> Hash[101100110101 Hash]; Hash -- Hash Encriptado usando Clave Privada --> Firma[Firma]
```

#### Verificación

```
graph TD; Firmado[Datos firmados digitalmente] --> Verificacion[Verificación]
```

Al ir hacia firmas, se muestra una vista donde también hay una pequeña explicación sobre la creación y verificación de firmas. El botón lleva a la vista donde se realizan estas funciones nombradas.

## Firma y Verificación

### Crear firma digital

Texto a firmar

Clave privada

```
CLAVE PRIVADA:
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
o
```

Resultado

[Firmar](#)

## Verificar firma digital

Texto a comprobar

Firma a validar

Clave pública

Comprobar

En esta vista están ambas funciones implementadas. Primero se creará una firma y después se verificará esa misma firma. Para acceder a un par de claves de forma rápida se puede acceder a <https://travistidwell.com/jsencrypt/demo/>

El mensaje a firmar será: ¡Hola, mundo!

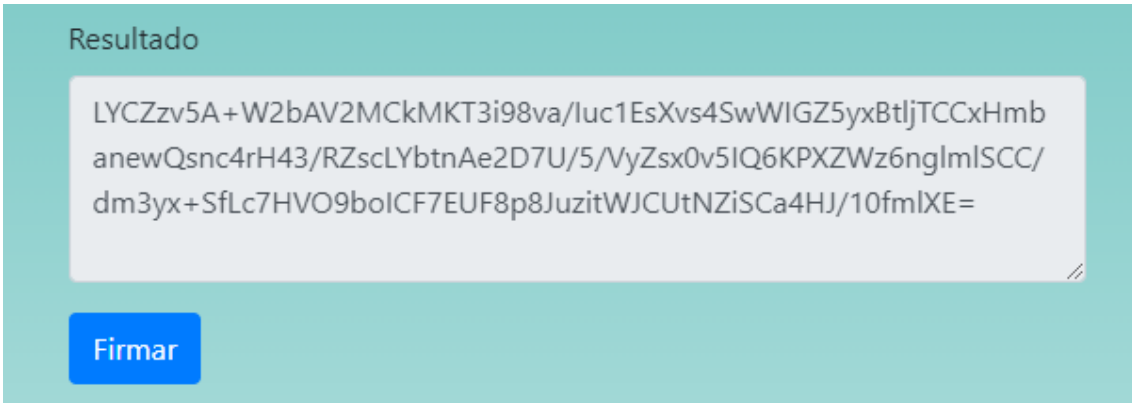
Primero se introduce el mensaje y la clave privada:

## Crear firma digital

Texto a firmar

Clave privada

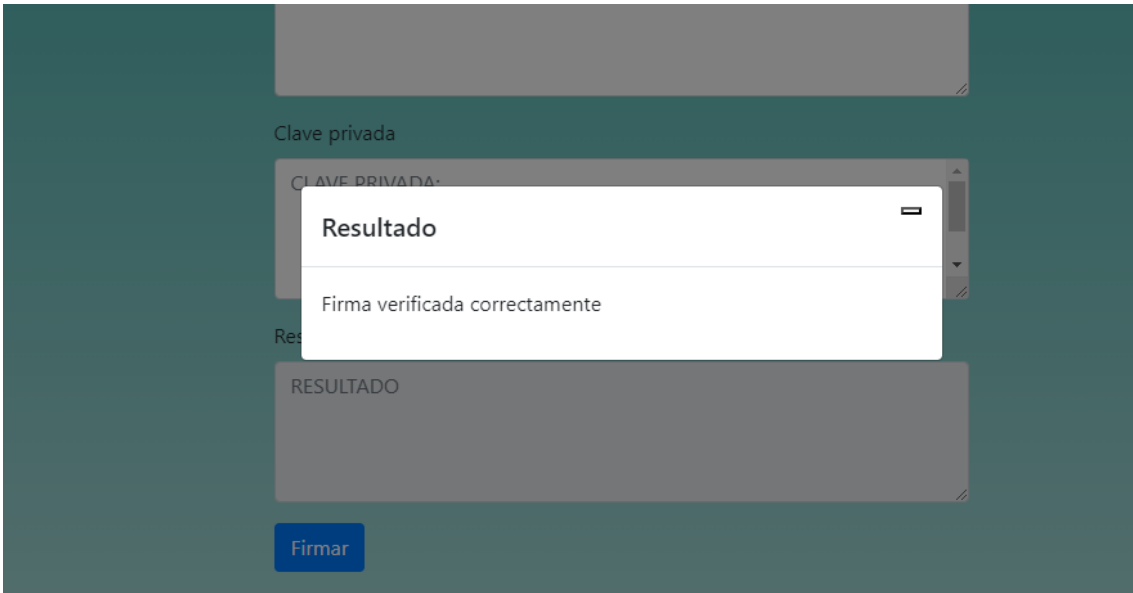
Y se firma:



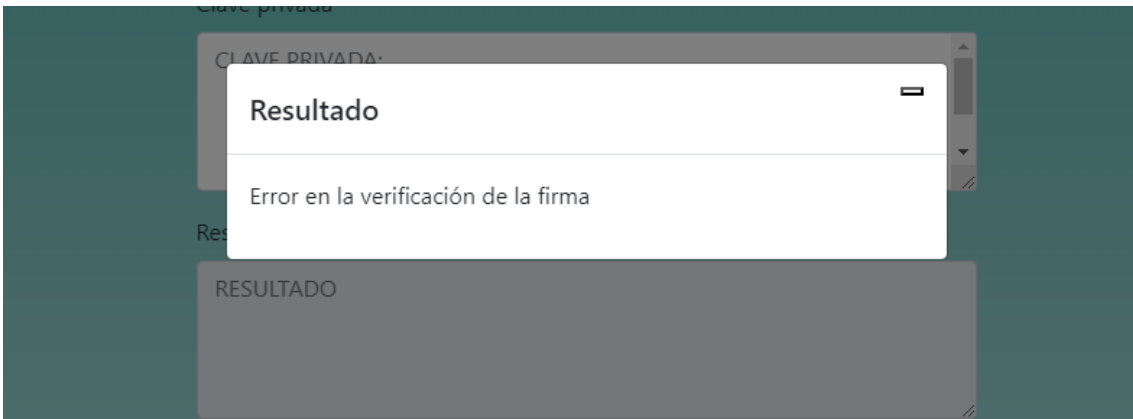
Ahora se comprueba la firma:



En la segunda función, tras introducir los datos y comprobar, si todo va bien, aparecerá el siguiente mensaje:



Si ha habido algún error, saldrá:



Fin del manual del usuario.