Anexo II

Análisis de requisitos y objetivos

Sistema de Prestación de Servicios de Certificación Electrónica

Trabajo de Fin de Grado

Grado en Ingeniería Informática

Autor

Tomás Calderón López

Tutor/a

Ángel Luis Sánchez Lázaro

Índice

1. Introducción

El objeto de este Anexo es crear y recoger los objetivos y requisitos que se van a cumplir para el éxito de este proyecto, estableciendo la base para la fase de desarrollo.

2. Participantes

A lo largo de este proyecto ha habido dos participantes, el tutor del trabajo Ángel Luis Sánchez Lázaro y el alumno y autor del trabajo, Tomás Calderón López.

Participante-01	Ángel Luis Sánchez Lázaro
Organización	Facultad de Ciencias de la Universidad de Salamanca
Rol	Tutor
Desarrollador	No
Cliente	No
Usuario	No

Participante-02	Tomás Calderón López
Organización	Facultad de Ciencias de la Universidad de Salamanca
Rol	Alumno
Desarrollador	Si
Cliente	Si
Usuario	Si

3. Objetivos

A continuación, se expondrán los objetivos generales y específicos del proyecto:

3.1. Generales

OBJ-01	Desarrollar un sistema de prestación de servicios de certificación electrónica

Versión	1
Autor	Tomás Calderón López
Descripción	El sistema deberá prestar un servicio web que permita al usuario, registrarse, autenticarse con credenciales y certificado, crear certificados personales y crear firmas digitales
Importancia	Muy alta
Sub-objetivos	OBJ-02

OBJ-02	Proporcionar información del procedimiento de configuración segura de Servidores Web
Versión	1
Autor	Tomás Calderón López
Descripción	El sistema deberá proporcionar información relacionada con los procedimientos llevados a cabo sobre la seguridad web y de los procesos relacionados con certificados y firmas digitales.
Importancia	Media
Sub-objetivos	

3.2. Específicos

OBJ-03	Gestionar el portal de manera segura
Versión	1
Autor	Tomás Calderón López
Descripción	La página web deberá poder utilizar HTTPS con un certificado para llevar a cabo sus comunicaciones con los clientes

Importancia	Alta
Sub-objetivos	OBJ-04 OBJ-05

OBJ-04	Validar la identidad de usuarios o identificarse con Certificados Personales
Versión	1
Autor	Tomás Calderón López
Descripción	La página web deberá poder autenticar a los usuarios del sistema tanto con credenciales como con certificados personales
Importancia	Muy alta
Sub-objetivos	

OBJ-05	Emitir certificados personales usando diferentes algoritmos criptográficos de clave pública
Versión	1
Autor	Tomás Calderón López
Descripción	La página web deberá poder emitir certificados personales para el uso de los usuarios del sistema
Importancia	Muy alta
Sub-objetivos	

OBJ-06	Generar y verificar firmas digitales basadas en Certificados
Versión	1
Autor	Tomás Calderón López
Descripción	La página web deberá poder crear y verificar firmas digitales a partir de un

	mensaje y una clave privada proporcionadas por el usario
Importancia	Media
Sub-objetivos	

OBJ-07	Registrar usuarios en el sistema
Versión	1
Autor	Tomás Calderón López
Descripción	La página web deberá permitir a cualquiera registrarse con un correo electrónico
Importancia	Muy alta
Sub-objetivos	

4. Requisitos del sistema

En esta sección se listarán los requisitos funcionales, que definen el comportamiento específico del sistema, y los no funcionales, que se centran en las características generales del sistema.

4.1. Requisitos funcionales

RF-01	Iniciar Sesión
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-04
Requisitos asociados	
Descripción	Los usuarios podrán autenticarse en el sistema con credenciales
Precondición	El usuario ha de estar registrado en el sistema
Secuencia	1. El usuario hace click en el login o es redirigido allí

	2. Introduce sus credenciales y los envía al sistema 3. El sistema los verifica, si son correctos crea una sesión, si no, lo redirige al inicio de sesión otra vez
Postcondición	El usuario está autenticado
Excepción	Fallo en la introducción de las credenciales

RF-02	Registro
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-07
Requisitos asociados	
Descripción	El usuario se registrará en el sistema mediante la introducción de credenciales y su email
Precondición	
Secuencia	1. El usuario entra en el registro 2. Introduce sus credenciales 3. Los envía al sistema y este los almacena
Postcondición	El usuario está registrado en el sistema
Excepción	Error si existe otro usuario ya registrado con el email proporcionado

RF-03	Verificar
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-01

Requisitos asociados	RF-02
Descripción	El usuario recibe un correo con un código de verificación
Precondición	Estar registrado en el sistema
Secuencia	1. Tras registrarse, el usuario recibe un correo con un enlace único para verificar su cuenta 2. Lo pulsa y el sistema lo verifica
Postcondición	El usuario está verificado y puede acceder a toda la funcionalidad del sistema
Excepción	

RF-04	Crear certificado personal
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-04 OBJ-05
Requisitos asociados	RF-03
Descripción	El usuario podrá crear un certificado, eligiendo los campos y el algoritmo
Precondición	Estar autenticado y verificado en el sistema
Secuencia	1. El usuario entra en Crear Certificados 2. Rellena los campos, escoge un algoritmo y presiona Crear certificado
Postcondición	Aparece el certificado en el almacén del usuario
Excepción	

RF-05	Descargar certificado
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-04 OBJ-05
Requisitos asociados	RF-03 RF-04
Descripción	El usuario podrá descargar el certificado desde su almacén en su perfil
Precondición	1. Estar autenticado y verificado 2. Haber creado un certificado
Secuencia	1. El usuario crea un certificado 2. Éste aparece en el almacén y el usuario lo descarga en el enlace
Postcondición	Se descarga el certificado personal con clave privada acoplada
Excepción	

RF-06	Iniciar sesión con certificado
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-01 OBJ-02 OBJ-04 OBJ-05
Requisitos asociados	RF-03 RF-04 RF-05
Descripción	El usuario se autentica en el servidor con un certificado personal

Precondición	1. Estar registrado y verificado en el sistema, pero no autenticado 2. Haber creado y descargado un certificado
Secuencia	1. El usuario instala el certificado personal del sitio web en el almacén de certificados (del sistema o del navegador) 2. Sin estar autenticado accede a la web, salta el "popup" de seleccionar certificado del navegador 3. El cliente escoge el suyo y se inicia sesión automáticamente
Postcondición	El usuario está autenticado
Excepción	

RF-07	Crear firma
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-06
Requisitos asociados	
Descripción	El usuario podrá crear una firma digital
Precondición	Estar autenticado y verificado
Secuencia	1. El usuario introduce un texto y una clave privada 2. El sistema crea la firma
Postcondición	Se crea una firma de unos datos
Excepción	

RF-08	Verificar firma

Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-06
Requisitos asociados	RF-07
Descripción	El usuario podrá verificar una firma digital
Precondición	Estar autenticado y verificado
Secuencia	1. El usuario introduce un texto, otro con la firma y una clave privada 2. El sistema comprueba si la firma es correcta o no
Postcondición	Se verifica la firma y se sabe si es correcto o no
Excepción	

RF-9	Cerrar Sesión
Versión	1
Autor	Tomás Calderón López
Objetivos asociados	OBJ-04
Requisitos asociados	RF-01 RF-06
Descripción	Los usuarios podrán cerrar sesión cuando estén autenticados
Precondición	Estar autenticado
Secuencia	1. El usuario cierra la sesión
Postcondición	El usuario deja de estar autenticado
Excepción	

4.2. Requisitos No Funcionales

RNF-01	Configuración segura
Versión	1

Autor	Tomás Calderón López
Objetivos asociados	OBJ-03
Descripción	El sistema deberá implementar una configuración de seguridad que incluye la activación de SSL/TLS y la habilitación de un certificado válido. Esto permitirá que el sitio web utilice HTTPS, garantizando una conexión segura y cifrada para los usuarios

5. Modelo de caso de uso

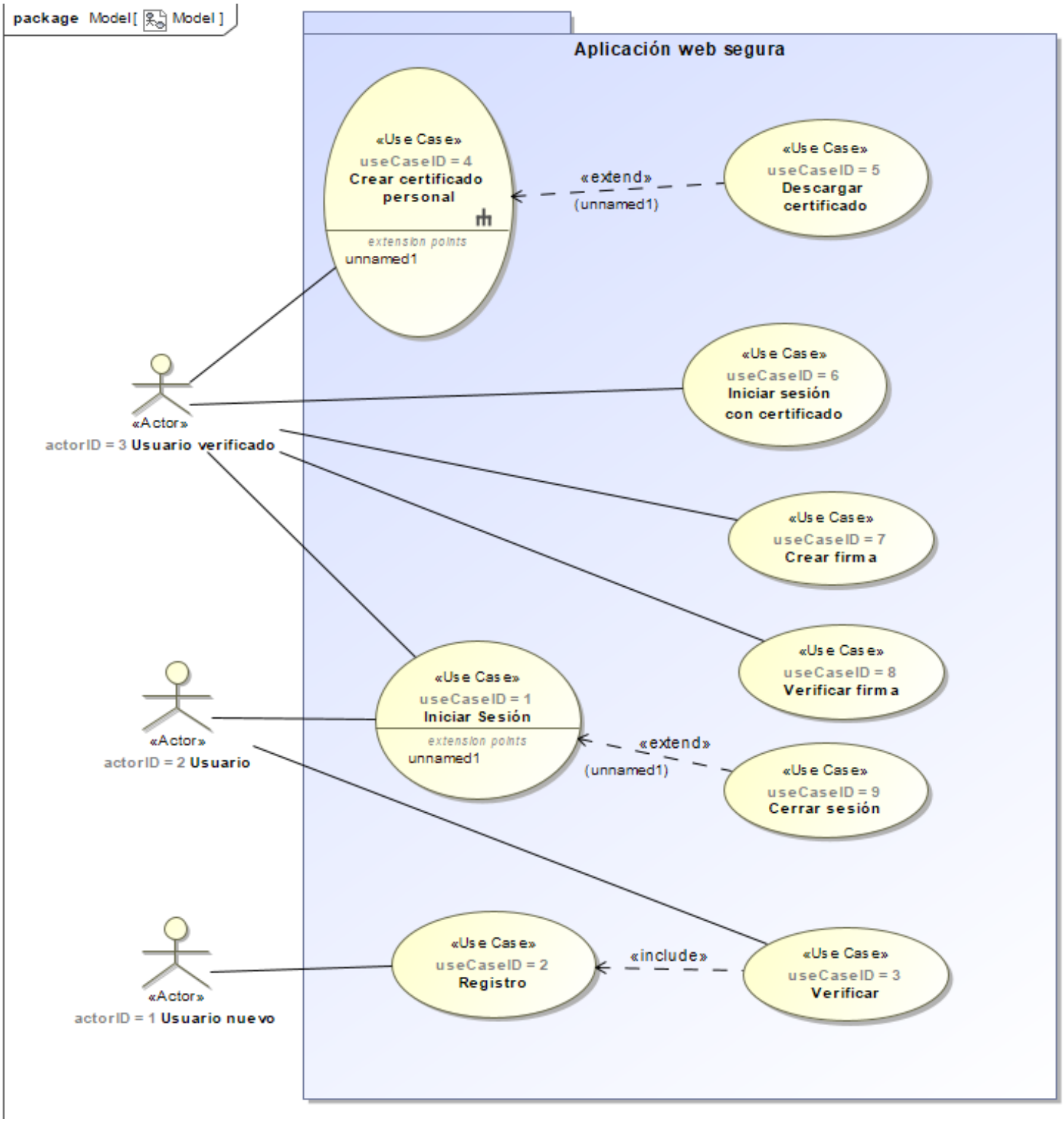
Una vez creados los requisitos, se muestra el diagrama de casos de uso relacionado con el sistema. Primero, los distintos actores que participan en el sistema:

ACT-01	Usuario sin registrar
Descripción	Nuevo usuario en la página que no está registrado en el sistema
Comentarios	

ACT-02	Usuario
Descripción	Usuario registrado y autenticado
Comentarios	

ACT-03	Usuario verificado
Descripción	Usuario registrado, autenticado y verificado con total acceso a las funciones del sistema
Comentarios	

Y el diagrama que representa el flujo de los casos de uso:


package Model [Model]
Aplicación web segura
«Use Case»
useCaseID = 4
Crear certificado personal
extension points
unnamed1
«extend»
(unnamed1)
«Use Case»
useCaseID = 5
Descargar certificado
«Use Case»
useCaseID = 6
Iniciar sesión con certificado
«Actor»
actorID = 3 Usuario verificado
«Use Case»
useCaseID = 7
Crear firma
«Use Case»
useCaseID = 8
Verificar firma
«Use Case»
useCaseID = 1
Iniciar Sesión
extension points
unnamed1
«extend»
(unnamed1)
«Use Case»
useCaseID = 9
Cerrar sesión
«Actor»
actorID = 2 Usuario
«Use Case»
useCaseID = 2
Registro
«include»
«Use Case»
useCaseID = 3
Verificar
«Actor»
actorID = 1 Usuario nuevo