

Escuela Técnica Superior de Ingeniería Informática

Ingeniería Informática

TRABAJO FIN DE CARRERA

Autoridad de Certificación: WebCA

Autor:

Jesús Fernández Sáez

Tutor:

Pablo Neira Ayuso

Curso 2017/2018

Índice

[Índice de figuras iii](#_Toc515315222)

[Índice de tablas iv](#_Toc515315223)

[1. Objetivo del proyecto 1](#_Toc515315224)

[2. Planificación del proyecto 1](#_Toc515315225)

[3. Introducción 2](#_Toc515315226)

[4. Solución propuesta 4](#_Toc515315227)

[5. Estado del arte 7](#_Toc515315228)

[5.1. Suites criptográficas 7](#_Toc515315229)

[5.2. Autoridades de certificación 7](#_Toc515315230)

[6. Criptografía de clave pública 9](#_Toc515315231)

[6.1. Glosario 9](#_Toc515315232)

[6.2. Generación de claves 10](#_Toc515315233)

[6.3. Estándares PKCS 12](#_Toc515315234)

[7. Infraestructuras de clave pública 14](#_Toc515315235)

[7.1. Estándar X.509 para certificados digitales 15](#_Toc515315236)

[7.2. Certificados digitales 15](#_Toc515315237)

[7.2.1. Estructura de un certificado 16](#_Toc515315238)

[7.2.2. Extensiones 17](#_Toc515315239)

[7.2.3. Formatos de archivo para certificados y PKI 18](#_Toc515315240)

[7.3. Cadenas de certificados 19](#_Toc515315241)

[7.3.1. Comprobación de la validez de un certificado 21](#_Toc515315242)

[7.3.2. Certificados autofirmados 22](#_Toc515315243)

[7.4. Validación cruzada de certificados 22](#_Toc515315244)

[7.5. Comprobación de la revocación de un certificado 24](#_Toc515315245)

[7.5.1. Listas de revocación de certificados – CRL 24](#_Toc515315246)

[7.5.2. Online Certificate Status Protocol – OCSP 25](#_Toc515315247)

[7.5.3. OCSP Stapling 26](#_Toc515315248)

[7.6. Autoridades de certificación 27](#_Toc515315249)

[7.6.1. Proceso de emisión de un certificado 28](#_Toc515315250)

[7.6.2. Tipos de CSR 29](#_Toc515315251)

[7.6.3. Distribución del certificado generado 30](#_Toc515315252)

[7.6.4. Seguridad relacionada con una CA 31](#_Toc515315253)

[7.7. Confianza en una PKI 31](#_Toc515315254)

[8. Requisitos del sistema 33](#_Toc515315255)

[8.1. Participantes 33](#_Toc515315256)

[8.1.1. Organizaciones participantes 33](#_Toc515315257)

[8.1.2. Personas participantes 33](#_Toc515315258)

[8.2. Objetivos del sistema 34](#_Toc515315259)

[8.3. Catálogo de requisitos del sistema 38](#_Toc515315260)

[8.3.1. Requisitos de información 38](#_Toc515315261)

[8.3.2. Requisitos de restricción 44](#_Toc515315262)

[8.3.3. Requisitos funcionales 48](#_Toc515315263)

[8.4. Matrices de rastreabilidad 97](#_Toc515315264)

[8.5. Análisis del sistema 103](#_Toc515315265)

[8.5.1. Tipos 103](#_Toc515315266)

[8.5.2. Tipos valor 111](#_Toc515315267)

[8.5.3. Asociaciones 116](#_Toc515315268)

[8.6. Operaciones del sistema 118](#_Toc515315269)

[8.6.1. Criptografía 118](#_Toc515315270)

[8.6.2. Plantillas 122](#_Toc515315271)

[8.6.3. Configuración CA 127](#_Toc515315272)

[8.6.4. Validaciones 132](#_Toc515315273)

[8.6.5. Usuarios 137](#_Toc515315274)

[9. Diseño de arquitectura 139](#_Toc515315275)

[9.1. Tecnología usada 139](#_Toc515315276)

[9.1.1. Programación de la capa servidor 139](#_Toc515315277)

[9.1.2. Programación de la capa cliente 142](#_Toc515315278)

[9.2. Arquitectura de la solución 143](#_Toc515315279)

[9.2.1. Componentes del sistema 143](#_Toc515315280)

[9.2.2. Certificados usados por el sistema 144](#_Toc515315281)

[9.2.3. Procesos del sistema 145](#_Toc515315282)

[9.3. Patrones de diseño 147](#_Toc515315283)

[10. Implementación 149](#_Toc515315284)

[10.1. Entorno de desarrollo 149](#_Toc515315285)

[10.2. Resultados del proyecto 149](#_Toc515315286)

[10.2.1. Estructura de la aplicación 149](#_Toc515315287)

[10.2.2. Estadísticas de creación 150](#_Toc515315288)

[10.3. Bases de datos 152](#_Toc515315289)

[10.4. Ejemplos del código desarrollado 152](#_Toc515315290)

[10.4.1. Autenticación de usuarios 152](#_Toc515315291)

[10.4.2. Modelos del sistema 153](#_Toc515315292)

[10.4.3. Respondedor OCSP 153](#_Toc515315293)

[11. Pruebas 155](#_Toc515315294)

[11.1. Pruebas unitarias 155](#_Toc515315295)

[11.2. Cobertura del código 155](#_Toc515315296)

[11.3. Testeo en Web CA 156](#_Toc515315297)

[12. Conclusiones y trabajos futuros 157](#_Toc515315298)

[13. Bibliografía 159](#_Toc515315299)

# Índice de figuras

[Figura 1. Arquitectura de alto nivel de la solución propuesta. 4](#_Toc515017824)

[Figura 2. La generación de claves RSA usa dos números primos muy grandes y, después de aplicar un algoritmo matemático, genera una pareja de claves. 10](#_Toc515017825)

[Figura 3. Ejemplos de jerarquías PKI con un certificado intermedio (izquierda) y con dos certificados intermedios (derecha). 14](#_Toc515017826)

[Figura 4. Información del certificado digital de www.openssl.org. 15](#_Toc515017827)

[Figura 5. Ejemplo de extensión SAN en el certificado de www.itu.int. 17](#_Toc515017828)

[Figura 6. Cadena de certificados para www.itu.int. 19](#_Toc515017829)

[Figura 7. El certificado final está firmado por un certificado intermedio COMODO RSA Extended Validation. 19](#_Toc515017830)

[Figura 8. El certificado intermedio está firmado por COMODO RSA Certification Authority. 19](#_Toc515017831)

[Figura 9. COMODO RSA Certification Authority es un certificado raíz ya que es autofirmado. 20](#_Toc515017832)

[Figura 10. Ejemplo de validación de una cadena de certificados. 21](#_Toc515017833)

[Figura 11. Validación cruzada entre PKI 1 y PKI 2. 22](#_Toc515017834)

[Figura 12. CRL de Starfield Secure Certificate Authority - G2. Detalles y certificados revocados. 24](#_Toc515017835)

[Figura 13. Esquema parcial de la jerarquía de certificados CA de la Fábrica Nacional de Moneda y Timbre (FNMT). 27](#_Toc515017836)

[Figura 14. Arquitectura de la solución implementada 141](#_Toc515017837)

[Figura 15. Certificados que usa Web CA para su funcionamiento 142](#_Toc515017838)

[Figura 16. Flujo de la autenticación con un código de un solo uso 143](#_Toc515017839)

[Figura 17. Flujo de la autenticación con claves criptográficas 143](#_Toc515017840)

[Figura 18. Proceso de emisión de un certificado 144](#_Toc515017841)

[Figura 19. Proceso de revocación de un certificado 144](#_Toc515017842)

[Figura 20. Número de líneas de código por lenguaje 148](#_Toc515017843)

[Figura 21. Modelos y relaciones de la base de datos de la web pública 149](#_Toc515017844)

# Índice de tablas

[Tabla 1. Implementaciones de Autoridades de Certificación disponibles. 7](#_Toc514965722)

[Tabla 2. Número de archivos por lenguaje de programación 147](#_Toc514965723)

# Objetivo del proyecto

Este proyecto consiste en la implementación de un software de Autoridad de Certificación que permite la implementación de una infraestructura de clave pública. Esta implementación de una CA usará los estándares habituales PKCS para la solicitud y emisión de los certificados, así como aquellos usados para comprobar la validez de un certificado. Esta implementación se centrará en la parte de usuario final y del administrador, es decir, en la fachada que permitirá realizar estas acciones de una manera sencilla y no se centrará en la implementación de todos los protocolos criptográficos usados. Para esto último se usará alguna de las suites criptográficas ya disponibles.

# Planificación del proyecto

Uno de los objetivos del proyecto es aprender a estimar el tiempo que se tarda en realizar cada una de las tareas que compone un proyecto de software.

A continuación, se muestra una tabla con las tareas a realizar durante el proyecto y con una estimación inicial del tiempo que requerirá cada tarea. También se puede observar el tiempo total empleado en la realización de cada tarea, así como el error en la estimación inicial.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tarea** | **Estimación inicial** | **Tiempo empleado** | **Error relativo** |
| Búsqueda y estudio de la documentación | 50 | 53 | 106% |
| Introducción y planificación | 60 | 77 | 128% |
| Requisitos | 40 | 74 | 185% |
| Instalación de la plataforma | 10 | 3 | 30% |
| Prototipo del diseño | 40 | 25 | 62% |
| Implementación | 250 | 183 | 78% |
| Revisión final de la documentación | 30 | 24 | 40% |
| **Total** | **480** | 442 |  |
| Error relativo medio |  |  | 89% |

El error relativo de cada tarea se calcula haciendo la razón entre el tiempo empleado y el tiempo estimado. Si ambos valores son iguales, será del 100%. Si se ha empleado más tiempo, será un valor mayor de 100% y querrá decir que se ha subestimado el tiempo que era necesario para hacer una tarea. El objetivo es estar lo más cerca posible del 100%.

# Introducción

Los certificados digitales son una parte fundamental de las comunicaciones seguras hoy en día. Casi cualquier servicio web ya usa el protocolo HTTPS para servir su contenido de una manera segura. Además, los certificados digitales tienen más aplicaciones que ayudar a hacer que un canal de comunicación sea seguro. La distribución o instalación de software habitualmente usa algún tipo de firma digital para que el usuario receptor de dicho software pueda confiar en que ha recibido una copia exacta a como el fabricante la haya publicado.

Así mismo, con la evolución de las sedes electrónicas de la Administración, todos los ciudadanos españoles disponen de su propio certificado digital en su DNI electrónico. En él se dispone de una serie de claves criptográficas y de varios certificados que permiten al ciudadano identificarse ante la Administración para hacer diferentes trámites como el pago de multas de circulación, obtención del certificado de nuestra vida laboral o hacer la declaración de la Renta.

Con el desarrollo de las tecnologías en la nube y servicios híbridos, muchas empresas también están haciendo uso de certificados digitales para la autenticación de sus usuarios. Por ejemplo, una empresa puede proporcionar a sus empleados un usuario y contraseña, pero también puede introducir un segundo factor de autenticación para asegurarse de que es el empleado el que realmente está intentando autenticarse. Este segundo factor puede ser un certificado digital en modo de certificado integrado en una smartcard de empleado o una smartcard virtual en el dispositivo del empleado. En ambos casos se trata de un certificado de usuario firmado habitualmente por la Autoridad de Certificación de la propia organización.

Un certificado digital es solo la parte más visible de las infraestructuras de clave pública. Dentro de una infraestructura de clave pública o PKI por sus siglas en inglés (Public Key Infrastructure) se tienen más conceptos como: clave privada, clave pública, firma digital o Autoridad de Certificación (CA). Estos conceptos se explicarán más adelante.

Existen varias implementaciones de suites criptográficas actualmente, algunas de código abierto y otras propietarias: OpenSSL, GnuTLS, NSS, CAPI2. Para este proyecto se ha elegido la librería OpenSSL ya que es una librería bien mantenida y usada frecuentemente en otras aplicaciones criptográficas por lo que asegura estar bajo revisión constantemente y soluciones relativamente rápidas para posibles vulnerabilidades que puedan surgir en el futuro. Además, existen adaptadores de esta librería para ser usada con una gran cantidad de lenguajes de programación.

El software que se va a desarrollar será una Autoridad de Certificación web, es decir, permitirá que un usuario pueda solicitar un certificado digital mediante una interfaz web, de manera que se facilite la solicitud, renovación o revocación de un certificado digital.

Los navegadores actuales soportan la creación de claves privadas directamente en el propio navegador por lo que la creación de una autoridad de certificación que solo necesite el uso de un navegador web sin ningún tipo de software adicional por parte de los usuarios simplifica enormemente estas tareas y está al alcance de cualquier usuario con un navegador que soporte estas operaciones. Por supuesto, se proporcionarán también funciones más avanzadas para la creación de certificados en el caso de que el usuario no disponga de un navegador que soporte estas funciones de clave privada.

Por otra parte, el uso de una aplicación web permite que la administración y configuración de un sistema sea más fácil al poderse usar desde cualquier tipo de dispositivo, ya sea fijo o móvil, además de ser independiente del sistema operativo del operador con lo que se imponen menos restricciones de este tipo. Además, es fácil escalar una aplicación web por lo que en caso de necesitar más capacidad para atender más peticiones de usuarios finales debería ser relativamente sencillo aumentar esta capacidad escalando horizontalmente, es decir, añadiendo más servidores web.

Finalmente, una parte importante de la comprobación de validez de los certificados digitales es poder contactar con la CA según una serie de protocolos como CRL y OCSP. CRL se simplifica cuando se usa un servidor web ya que estas listas se publican habitualmente en archivos descargables y es sencillo cuando ya se dispone de un servidor web. OCSP es un protocolo puramente HTTP.

# Solución propuesta

La solución que se propone es una aplicación web que permitirá a un usuario final realizar las siguientes acciones principales, entre otras:

* Solicitar un certificado digital. La CA debe realizar algún tipo de comprobación de los datos que el usuario proporciona, según el tipo de certificado digital que se solicite.
* Renovar un certificado digital. Dado que los certificados digitales tienen un periodo de validez, una vez que este expire, el usuario puede solicitar que el certificado se vuelva a emitir para un nuevo periodo de validez.
* Revocar un certificado. En determinadas circunstancias se podría necesitar que un certificado deje de ser válido por lo que se tiene que permitir que un usuario solicite dar de baja un certificado y la CA debe incluirlo dentro de sus listas de revocación de certificados como certificado no válido.

Un operador que administre la CA podrá hacer las siguientes acciones:

* Realizar tareas durante la creación de los certificados. Estas tareas pueden ser aprobar o denegar la emisión de un certificado o revocar un certificado unilateralmente.
* Administrar las plantillas de certificados que los usuarios pueden usar. Dado que los certificados tienen diferentes usos, tiene sentido la creación de plantillas que especifiquen los diferentes certificados que la CA puede emitir. Ejemplos de plantillas pueden ser: certificados de usuario para autenticación, firmado o cifrado de correos electrónicos, certificados para servidores (web, correo, etcétera) o certificados para firmado de software.

La arquitectura de la solución será:

* Una aplicación web para los usuarios. Esta será el punto de acceso público a la Autoridad de Certificación.
* Una aplicación web para los administradores. Al tener su propia aplicación web, se puede restringir el acceso a esa aplicación de una manera diferente a la pública, ya sea por restricción de IP, método de autenticación, etc.
* Una aplicación web para la publicación de listas de revocación de certificados (CRL), así como un respondedor OCSP para atender este tipo de peticiones de validación.
* Un proceso emisor (servicio en modo demonio) que se encargará de realizar las tareas de cifrado/firmado de certificados pendientes. Este servicio leerá de una cola de acciones pendientes y actualizará las acciones pendientes con el resultado. Al tener un proceso separado del servicio web, se puede restringir el acceso a la clave privada de la CA que es la parte más importante de toda la CA. Este servicio puede ejecutarse en las mismas máquinas que las aplicaciones web o no.
* Un sistema de almacenamiento para los usuarios finales de la CA. Se podría usar un directorio LDAP si esta se despliega en una organización con un directorio LDAP.
* Un sistema de almacenamiento para los usuarios de administración. Igual que en el caso anterior, también se podría usar un directorio LDAP para identificar estos usuarios.

La arquitectura de la aplicación está descrita en la siguiente figura.

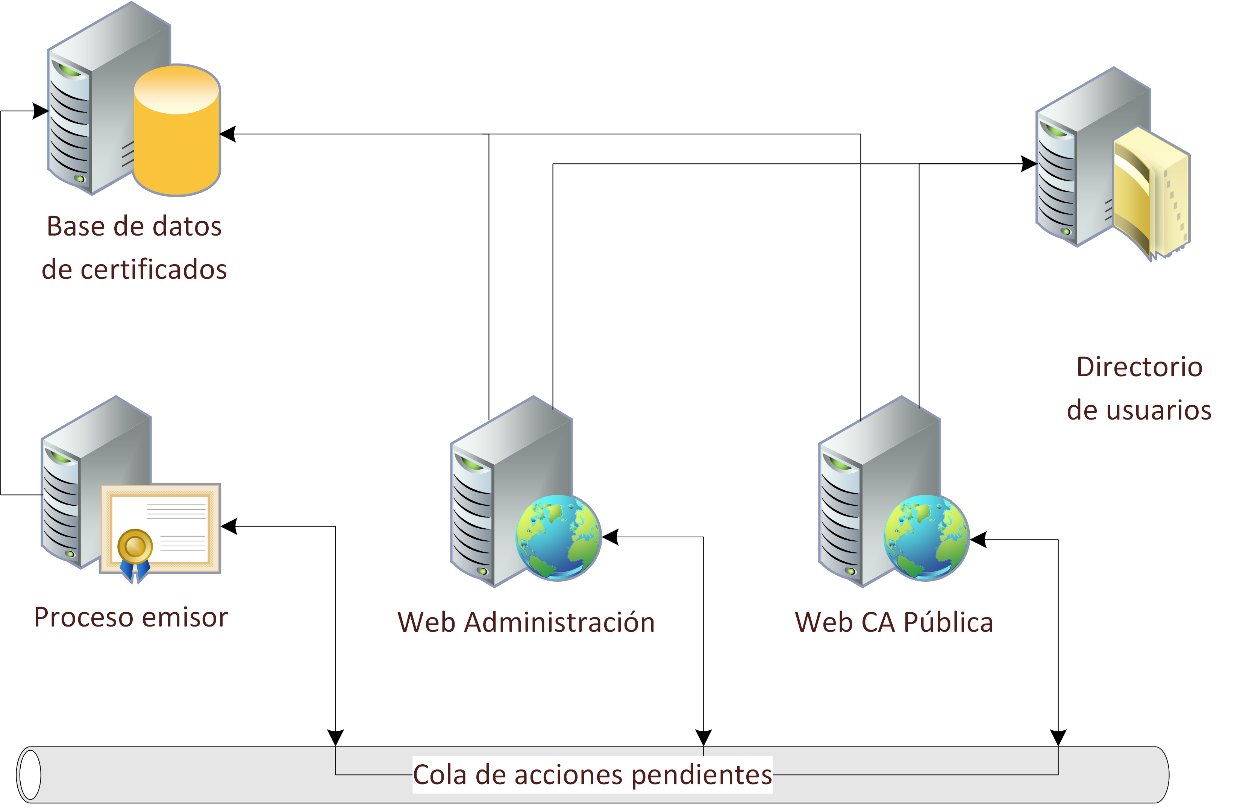


Figura 1. Arquitectura de alto nivel de la solución propuesta.

Se ha elegido Python como lenguaje de programación para el desarrollo de la parte de servidor de la aplicación. Python es un lenguaje de programación versátil y potente, pero también sencillo de leer y fácil de usar. Ha crecido mucho en popularidad en los últimos tiempos y, al ser un lenguaje derivado de C, es un lenguaje sencillo al que adaptarse.

Python dispone de uno de los framework de desarrollo web más conocidos: Django. Django dispone de una serie de características que lo hacen muy atractivo:

* MVC: sigue el principio Modelo-Vista-Controlador que permite separar la aplicación en estas tres conocidas capas. Una arquitectura MVC separa la lógica de la aplicación en tres capas: el modelo abstrae los datos que maneja el sistema, la vista es la interfaz de usuario y el controlador es la capa intermedia entre modelo y vista que gestiona la adaptación entre uno y otro. En el caso de Django, el modelo se corresponde con las clases que se definen para almacenar datos en las bases de datos, pero la línea entre la vista y controlador es más difusa. En Django, los datos (modelos) se procesan con Vistas y se renderizan usando Plantillas.

En el contexto de este proyecto, los modelos gestionan la información de la aplicación, por ejemplo, solicitudes de certificados, certificados emitidos y plantillas de certificados o usuarios y grupos. Las vistas de Django se usan para ver qué modelos hay que presentar según el caso de uso y con las plantillas se renderiza siempre una página web.

* ORM: Object Relational Mapper, interactuar con los modelos de base de datos es extremadamente sencillo usando el ORM que incorpora Django. Esta capa de abstracción permite desarrollar la aplicación sin necesidad de hacer consultas a las bases de datos directamente e independientemente del sistema de base de datos que haya por debajo.
* Migración de modelos: dado que una aplicación puede ir evolucionando con el tiempo, así mismo lo pueden hacer sus modelos (entidades que se guardan en base de datos). Django incorpora un sistema de migración y actualización de modelos que hace los cambios necesarios en los esquemas de las bases de datos.

# Estado del arte

A continuación, se muestran primero las diferentes implementaciones de librerías para trabajar con funciones criptográficas y certificados y posteriormente se muestran algunas implementaciones de software para crear una autoridad de certificación.

## Suites criptográficas

Todos los lenguajes de programación habituales tienen implementaciones para trabajar con certificados X.509, ya sea mediante implementaciones directas de o envolviendo otras librerías como OpenSSL.

OpenSSL es una implementación de código abierto de los protocolos SSL y TLS hecha en C. Muchas de las librerías disponibles para el resto de los lenguajes de programación se basan en llamar al código de OpenSSL para realizar operaciones. Además de ser una librería, OpenSSL incluye una serie de aplicaciones de consola para administrar claves, certificados, generar CSR e incluso cifrar datos. LibreSSL y BoringSSL son otros proyectos derivados de OpenSSL.

Otra librería libre es GnuTLS, que tiene una lista de funcionalidades similar.

Para la plataforma Windows y sus lenguajes de programación, Microsoft tiene su propia implementación de los protocolos y funciones de criptografía llamada CryptoAPI o CAPI, aunque es una librería propietaria.

## Autoridades de certificación

Existen varias implementaciones de código abierto. La mayoría implementan los servicios más habituales como emisión, revocación y administración de certificados digitales, es decir, X.509, CSR y CRL.

Debido a que OpenSSL es una de las librerías de código abierto más utilizadas, muchas de las implementaciones disponibles usan esta librería para las operaciones criptográficas.

En la Tabla 1 se comparan algunas de las implementaciones disponibles más notables. Como se podrá ver, la fecha de las últimas versiones estables de la gran mayoría no es realmente reciente. Todas las implementaciones escogidas son multiplataforma.

De las diferentes Autoridades de Certificación de código abierto que existen, sin duda, EJBCA es la CA que aparentemente está más usada. Por una parte, tiene una versión Community que cualquiera puede descargar y crear su propia CA. Existe también una versión comercial llamada Enterprise orientada a organizaciones donde ya se da soporte por parte de una empresa dedicada a seguridad informática. Es además un software que puede ser extendido por el usuario y existe diferente software complementario para que EJBCA pueda ampliar sus funcionalidades como el uso de tokens hardware o poder usarlo con smartcards.

XCA ha sido actualizada muy recientemente después de 3 años de inactividad. Además del uso básico para generar certificados digitales, se puede usar también con smartcards o tokens USB si se instala una librería compatible. Conviene decir que esta CA es una aplicación de escritorio y no tiene una versión web, por lo que su uso queda limitado al PC donde está instalada.

Igual que XCA, gnoMint es otra CA cuya interfaz es una aplicación de escritorio o una interfaz de consola, por lo que tampoco se puede interactuar con ella mediante una web. gnoMint soporta el únicamente la administración básica de una CA y la creación/revocación de certificados. Y de nuevo, al igual que XCA, gnoMint no publica CRLs o tiene un respondedor OCSP, aunque sí soporta la configuración de rutas CRL/OCSP en los certificados que genera. Para estas funcionalidades depende software externo.

OpenCA es un conjunto de proyectos relacionados con autoridades de certificación y en el que uno de estos proyectos es una CA. La arquitectura de esta CA es distribuida y soporta tanto una CA offline como una RA online (Registration Authority). Esta CA sí tiene una interfaz web y soporta CRLs y OCSP.

Finalmente, la única CA digna de mención cuyo lenguaje es Python es pyCA. Esta es una CA offline y cuyas funcionalidades están basadas en el uso de scripts de consola y tareas programadas. Se podría decir que el proyecto está muerto ya que la última versión disponible data de 2003.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre | Licencia | Lenguaje | Versión estable | Notas |
| EJBCA | LGPL v2.1 | Java  J2EE | Diciembre 2017 | Implementa OCSP, CMP,  XKMS, SCEP, EC y CVC  (pasaportes digitales)  Clusterizable  Tiene un modo, usar y tirar, donde nada queda registrado y es capaz de generar una gran cantidad de certificados muy rápidamente.  CC, PP EAL4+[[1]](#footnote-2) |
| gnoMint | GPL v3 | C | Marzo 2016 |  |
| OpenCA PKI | GPL | Perl | Agosto 2013 | Basada en OpenSSL.  OCSP, SCEP.  Distribuible.  Interfaz web. |
| r509 | Apache 2.0 | Ruby | Diciembre 2016 | Basada en OpenSSL.  OCSP, SPKI/SPKAC.  Interfaz web. |
| TinyCA | GPL | Perl | Marzo 2007 | Basada en OpenSSL. |
| XCA | BSD | C++ | Enero 2018 |  |
| pyCA | GPL | Python | Noviembre 2003 |  |
| newPKI | GPLv2 | C++ | Diciembre 2005 | Basada en OpenSSL |

Tabla 1. Implementaciones de Autoridades de Certificación disponibles.

# Criptografía de clave pública

La criptografía de clave pública también se conoce como criptografía asimétrica [1]. La criptografía simétrica usa una única clave conocida y compartida por las dos partes de una comunicación. En cambio, la criptografía asimétrica usa algoritmos criptográficos que requieren dos claves para su funcionamiento, una para cifrar y otra descifrar. En este tipo de algoritmos, una de las claves es de dominio público, llamada clave pública, mientras que su pareja, la clave privada, se debe mantener, como su nombre indica, de manera privada. La clave pública se usa para cifrar o comprobar la validez de una firma digital, mientras que la clave privada se usa para descifrar o para generar una firma digital.

La criptografía de clave pública tiene dos usos habituales:

* Confidencialidad: solo el receptor del mensaje puede ver el contenido de este. Como se explica en el párrafo anterior, un mensaje se cifra con la clave pública y solo el poseedor de la clave privada puede descifrar dicho mensaje.
* Autenticación: el receptor sabe a ciencia cierta que el emisor del mensaje es quien dice ser. Es decir, existe un mecanismo que permite al receptor saber quién envió el mensaje. En el caso de certificados digitales se trata de una firma digital. La firma se crea con la clave privada, de manera que cualquiera que posea la clave pública puede confirmar que la firma es correcta. Además, la firma depende del contenido del mensaje, por lo que validar que la firma es correcta asegura que el mensaje solo puede haber sido firmado por quien tiene la clave privada y que el contenido del mensaje no ha sido modificado.

## Glosario

Para entender el funcionamiento de una PKI se necesita conocer el significado de algunos conceptos básicos, aunque alguno se explicará con más detalle en posteriores epígrafes:

* Clave privada

Clave que se mantiene en secreto y que se usa para descifrar un mensaje o para crear una firma digital.

* Clave pública

Clave conocida públicamente que se usa para cifrar un mensaje o para comprobar la validez de una firma digital.

* Pareja de claves

Una pareja de claves está formada por una clave pública y por una clave privada. Estas se generan habitualmente en el mismo momento según un determinado algoritmo. Dan lugar a lo que se llama criptografía asimétrica: con una clave se cifra y solo con la otra se puede descifrar y viceversa.

* Función hash

Función hash o función resumen. Es un algoritmo al que se le pasa como entrada la representación de un objeto de longitud indeterminada y habitualmente devuelve una cadena de caracteres con una longitud determinada que se puede usar como resumen de dicho objeto. Cualquier mínima modificación de la cadena original y, por tanto, del objeto original, debe hacer que la función hash tenga una salida diferente. Son funciones de un único sentido, es decir, una vez computado el resumen de un objeto, debe ser muy difícil conseguir el objeto original.

* Firma digital

Mecanismo en el que se usa la clave privada para cifrar el hash de un objeto. Con la firma se proporciona el hash original y el hash cifrado (firmado) de manera que cualquier usuario dispone de la clave pública para poder descifrar el hash firmado y comprobar que es el mismo que el original. Dado que solo el firmante tiene la clave privada, se puede comprobar así la autenticidad de la firma.

* Certificado digital

Documento digital que incluye una clave pública, una serie de datos sobre el propietario de la clave pública, un periodo de validez y la firma digital de dicho certificado realizada por una determinada entidad. Esta firma digital asegura que una Autoridad de Certificación da los datos que presenta el certificado digital como válidos.

Un certificado también puede ser autofirmado, es decir, que está firmado por la propia clave privada correspondiente a la clave pública del certificado.

* Autoridad de Certificación

El cometido principal de una Autoridad de Certificación o CA es firmar un certificado digital después de comprobar la validez de los datos del solicitante. Los usuarios de ese certificado digital, al confiar esta CA darán por válido los certificados que esta CA firme.

Una CA tiene su propia pareja de claves y certificado firmado por otra CA diferente. Si el certificado de una CA es autofirmado, entonces se dice que es una Autoridad de Certificación Raíz.

* Cadena de confianza

Simplificando los conceptos, un certificado digital está firmado por el certificado de una CA. El certificado de esta CA está firmado por otra CA superior. Esta cadena de firmas digitales forma una cadena de confianza. Las CA que están arriba del todo en la jerarquía son las CA que tienen certificados autofirmados, es decir, son las CA Raíz. Los usuarios habitualmente confían en las CA Raíz de manera que, al confiar en la que está arriba del todo, un usuario puede confiar en todos los certificados intermedios o finales cuya cadena de confianza empiece por ese certificado raíz.

## Generación de claves

Existen varios algoritmos para generar parejas de claves. Estos algoritmos se basan en problemas matemáticos que tienen una solución costosa de obtener en un tiempo razonable. Debe ser fácil generar la pareja de claves, pero debe ser muy costoso computacionalmente deducir la clave privada a partir de la clave pública ya que esta va a ser distribuida y no es secreta.

Es necesario que las claves sean generadas con la mayor aleatoriedad y entropía posible. En el RFC 4086[[2]](#footnote-3) describe una serie de requerimientos necesarios de garantizar un nivel de aleatoriedad suficiente. En la práctica, las claves son números primos de muchos dígitos. Estos se podrían generar de diferentes maneras:

* Usando un generador de números aleatorios o pseudoaleatorios.
* Con una *frase de paso* a la que se le aplica una función de *hash*.

Las implementaciones de criptografía asimétrica más usadas actualmente se pueden encontrar en la siguiente lista. Existen otros métodos para generar una pareja de claves, pero los descritos en la lista son los que se usan con más frecuencia. Cada protocolo usa un algoritmo propio para generar una pareja de claves.

* RSA. Se basa en la dificultad de factorizar el producto de dos números primos grandes. Se hizo público por primera vez en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman y de ahí su nombre. Las recomendaciones para su implementación están recogidas en PKCS #1[[3]](#footnote-4).

Una pareja de claves RSA se puede usar tanto para cifrar y como para crear firmas digitales.

Para RSA, las claves actuales suelen tener un tamaño entre 1024 bits y 4096 bits. Menos de esto se considera inseguro. Dado que una clave de 768 bits fue rota en 2009[[4]](#footnote-5), en la actualidad se recomienda usar claves de 2048 bits o mayores ya que debido a los avances actuales no está claro si algunas agencias de inteligencia son ya capaces de romper una clave de 1024 bits.

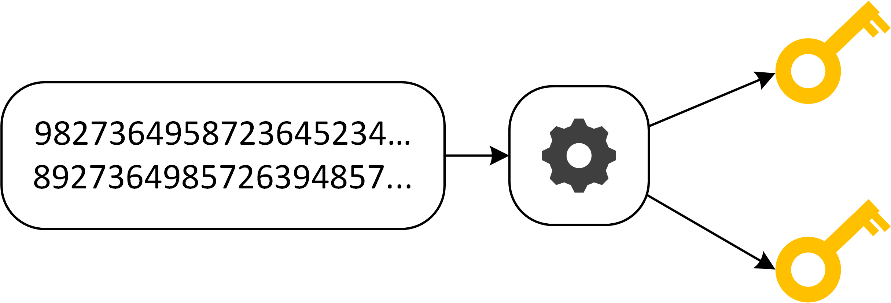


Figura 2. La generación de claves RSA usa dos números primos muy grandes y, después de aplicar un algoritmo matemático, genera una pareja de claves.

* ElGamal. Otro sistema de cifrado asimétrico que se basa en un problema matemático diferente al sistema RSA. En este caso, la seguridad se basa en la dificultad de computar logaritmos discretos. ElGamal usa un intercambio de claves Diffie-Hellman. Publicado por Taher ElGamal en 1985[[5]](#footnote-6). Existe otro algoritmo llamado ElGamal del mismo autor, pero usado para firmas digitales y muy poco usado en la práctica, pero es en el que se basa el protocolo DSA descrito en el punto siguiente.

Es uno de los algoritmos que se puede usar en GnuPG[[6]](#footnote-7), una implementación GNU de PGP, del que hablaremos más adelante.

* DSA, Digital Signature Algorithm. Es una variante del sistema de firma ElGamal. Este sistema se basa en la dificultad de computar logaritmos discretos. Desarrollado por la NSA y publicado por primera vez en 1991, fue patentado por el NIST (National Institute of Standards and Technology de EE. UU.) y adoptado como FIPS (Federal Information Processing Standards) 186 en 1993[[7]](#footnote-8).

FIPS-186 especifica que también se puede usar una pareja de claves RSA para firmas digitales con la restricción de que esta pareja de claves solo se use con el propósito de firma digital.

Al igual que en el caso de claves RSA para cifrado, se recomiendan claves de 2048 bits o mayores.

Como se ha visto, las claves tienen un tamaño que se expresa en bits. A mayor número de bits, la clave será más grande y, por consiguiente, más difícil de romper. La criptografía asimétrica necesita tamaños de clave mayores que la criptografía simétrica para ofrecer el mismo nivel de seguridad. Por ejemplo, NIST se estima que una clave RSA de 15360 bits es comparable a una clave simétrica AES de 256 bits[[8]](#footnote-9). Existen algoritmos asimétricos basados en curvas elípticas (ECC o Elliptic Curve Cryptography) que parecen ser seguros con claves más cortas[[9]](#footnote-10). Por ejemplo, una clave ECC de 224 bits se puede comparar con una clave simétrica de 112 bits, también según el NIST.

## Estándares PKCS

PKCS son las siglas de Public Key Cryptography Standard. En PKCS se recogen una serie de estándares relacionados con la criptografía de clave pública. RSA Security Inc. inició la publicación de estos estándares para promover el uso de los algoritmos criptográficos patentados por la compañía. Algunos de estos estándares se usan actualmente, aunque algunos hayan sido abandonados o sustituidos por otros. En la siguiente lista se describen brevemente aquellos estándares PKCS aún en uso [2]:

* PKCS #1, RSA Cryptography Standard, comentado anteriormente y donde se define la criptografía RSA. Las claves privadas se escriben usando la notación ASN.1 [3]. Publicado en el RFC 8017.
* PKCS #3, Diffie-Hellman Key Agreement Standard, donde se define el intercambio de claves Diffie-Hellman, un protocolo con el que dos interlocutores que no se conocen pueden conseguir establecer una clave secreta compartida en un canal de comunicación no seguro.
* PKCS #5, Password-based Encryption Standard, donde se define un estándar de cifrado basado en contraseñas. Publicado en el RFC 8018.
* PKCS #7, Cryptographic Message Syntax Standard. Precursor del S/MIME y usado para cifrar o firmar mensajes, así como para la distribución de certificados en una PKI. Publicado en el RFC 2315.
* PKCS #8, Private-Key Information Syntax Standard, donde se define un estándar usado para transportar parejas de claves, cifradas o sin cifrar. Publicado en el RFC 5958.
* PKCS #9, Selected Attribute Types, donde se definen tipos de atributos para usar en certificados PKCS #6, mensajes firmados PKCS #7, claves privadas PKCS #8 y solicitudes de firma de certificados PKCS #10. Publicado en el RFC 2985.
* PKCS #10, Certification Request Standard. Define el formato de los mensajes que se deben enviar a una autoridad de certificación para solicitar un certificado. Publicado en RFC 2986.
* PKCS #11, Cryptographic Token Interface. También conocido como "Cryptoki", es una API que define métodos genéricos para interactuar con un dispositivo token criptográfico, que son módulos criptográficos en hardware como, por ejemplo, una smart card (DNIe [4]).
* PKCS #12, Personal Information Exchange Syntax Standard, define un formato de archivo usado para almacenar claves privadas y sus certificados, protegidos por una clave simétrica. Es una evolución de PFX. Publicado en RFC 7292.
* PKCS #15, Cryptographic Token Information Format Standard, que define un mecanismo para que un usuario pueda usar un token criptográfico ante aplicaciones que sigan estos estándares, independientemente del proveedor o interfaz de este token.

# Infraestructuras de clave pública

Ahora que se sabe en qué se basa la criptografía de clave pública: se debe tener una pareja de claves, una privada y una pública. Si es necesario que una persona envíe un documento cifrado para que solo otra pueda leerlo, la persona que lo envía debe la clave pública de la que lo recibe para cifrar dicho documento. De esa manera, solo el que lo recibe con su clave privada puede descifrar ese mensaje que le llega.

Por otra parte, si una persona quiere enviar un documento asegurando a la que lo recibe que ha sido ella quien lo ha enviado y que nadie durante la transmisión ha modificado ese documento, el emisor firma digitalmente el mensaje con su clave privada y envía la firma junto al documento. De esa manera, cuando la otra persona reciba el documento y la firma, podrá comprobar con la clave pública del emisor la validez de la firma digital y podrá confiar en que el documento que le ha llegado es idéntico al que el otro había enviado.

Pero ¿cómo es posible estar seguro de que la clave pública que se recibe es efectivamente de la persona a la que se quiere enviar un documento secreto? Evidentemente una manera sería ir físicamente donde esté esa persona y que él mismo nos dé su clave pública. En la práctica, esta no es una solución viable ya que la persona no tiene por qué estar en la misma ciudad que nosotros, o ni siquiera en el mismo país.

Para solucionar este problema se introduce el concepto de confianza. ¿Qué permite a un usuario confiar en que la clave pública que tiene corresponde con la persona con la que se está comunicando o servicio al que quiere acceder? Hay dos respuestas a esta pregunta:

* Que las claves públicas que vayamos a usar estén firmadas por un ente u organismo central en el que el usuario confíe.
* Que las claves estén firmadas por otro individuo (o un grupo de individuos) en el que el usuario confíe.

Estas dos respuestas dan lugar a los dos grandes modelos de infraestructuras de clave pública que se usan en la actualidad: un modelo PKI centralizado o un modelo descentralizado, también conocido como *Web of trust* o anillo de confianza.

En el primer caso de una PKI centralizada, existen una o varias autoridades organizadas en una jerarquía que firman las claves públicas de los usuarios. Si se confía en la autoridad de nivel superior, por defecto, se confiará en todos los certificados que sean firmados por ella u otras autoridades que estén por debajo de la de nivel superior. Esto permite crear una relación de confianza con un gran número de certificados con tan solo confiar en una única entidad.

En el caso del anillo de confianza, esta autoridad de nivel superior no existe en un principio. Cada usuario tiene su pareja de claves y un anillo de claves públicas en las que confía. La confianza se crea cuando un usuario firma la clave pública de otro usuario. Así, se podría confiar en que una clave pública determinada corresponde con seguridad a su propietario sabiendo cuántas personas o entidades han firmado dicha clave.

Un usuario normal usará la mayor parte de su vida una infraestructura centralizada, sabiéndolo o no, ya que es la que se usa mayoritariamente para la navegación web. Para que un usuario normal no tenga que pasar por el proceso de confiar en las autoridades de certificación, actualmente los diferentes sistemas operativos y navegadores incluyen una serie de certificados en los que ellos confían y, por tanto, en las que sus usuarios confiarán. Esto no impide no obstante que un usuario pueda decidir si confiar o no en estas entidades. Dependiendo del sistema operativo, el usuario puede eliminar (o añadir) las entidades en las que confía.

## Estándar X.509 para certificados digitales

El estándar X.509 es un estándar ITU-T para PKI y para PMI (Privilege Management Infrastructure).

Pensado originalmente como complemento al estándar X.500 en su faceta de autenticación, este estándar fue adoptado fuera del estándar X.500En este estándar se definen formatos para certificados de clave pública, listas de revocación de certificados (CRL), certificados de autorización (relacionados con PMI), así como un algoritmo para comprobar la validez de la cadena de certificados. La última versión publicada de este estándar es la Versión 3, publicada en el RFC 5280 [5], siendo el RFC 3280 [6] la versión inicial y el RFC 6818 [7] la última corrección o actualización del estándar.

Al igual que el estándar X.500 para servicios de directorios, el X.509 se basa en una jerarquía estricta de autoridades de certificación (CA) para la emisión de certificados digitales. Por tanto, nos encontramos con una infraestructura centralizada como de la que hablábamos en el epígrafe anterior. Aquellas CA que están en lo más alto de la jerarquía se llaman Autoridades de Certificación Raíz y son las que suelen estar incluidas en los sistemas operativos y navegadores web. Si pensamos en esta jerarquía como un árbol, en la raíz de la jerarquía está el certificado de la CA Raíz y en las hojas están los certificaos finales que serán usadas por los servidores o lo usuarios para su autenticación. Los nodos intermedios en el árbol son las llamadas CA intermedias. Se considera una buena práctica que los certificados finales sean emitidos por CA intermedias, en vez que por una CA raíz. De esa manera, si un certificado intermedio se ve comprometido, solo es necesario cortar esa rama del árbol. Si un certificado raíz se viera comprometido, entonces habría que cortar todo el árbol con el consiguiente *trauma* que ello podría conllevar.

|  |  |
| --- | --- |
|  |  |

Figura 3. Ejemplos de jerarquías PKI con un certificado intermedio (izquierda) y con dos certificados intermedios (derecha).

## Certificados digitales

Un certificado digital consiste en asociar una clave pública con una serie de detalles adicionales como son:

* A qué persona u organización identifica dicho certificado.
* Quién firma el certificado, es decir, quién asegura que el certificado es del propietario.
* Las fechas desde la que es válido el certificado y la fecha en la que expira.
* Para qué usos está aprobado puede usar el certificado.

El uso más visible de los certificados digitales para un usuario es el de crear una conexión segura a la hora de navegar por Internet. Es usado en conjunto con el protocolo TLS (Transport Layer Security) y permite al usuario confiar en que se está conectando al servidor que pretendía conectarse y, además, tener relativa seguridad de que nadie puede interceptar esa comunicación con el servidor y que queda en secreto entre el usuario y el servidor.

Los certificados pueden estar asociados a nombres de Internet (DNS), en el caso de sitios web, pero también pueden estar asociados a direcciones de correo electrónico o cuentas de usuario de algún servicio de directorio determinado. Es lo que se conocen como certificados de usuario y pueden usarse para cifrar/firmar comunicaciones por correo electrónico o para firmar software, por ejemplo.

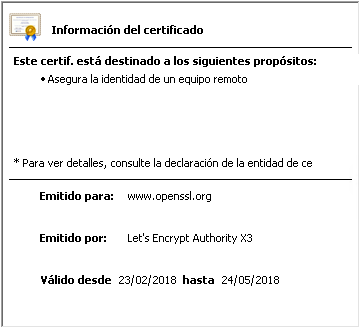


Figura 4. Información del certificado digital de www.openssl.org.

En el caso de una PKIX (PKI X.509), los certificados digitales están asociados a un nombre distinguido (Distinguished Name) del estilo X.500, o bien a un nombre alternativo como una dirección de correo electrónico o una entrada DNS. Una CA firma con su propio certificado un certificado que está expidiendo, de manera que cualquier usuario que confíe en la CA (o su CA raíz) confiará en el nuevo certificado.

### Estructura de un certificado

Los certificados X.509v3 se expresan según la notación ASN.1 definida en el PKCS #1. El RFC 5280 define la estructura de un certificado y una serie de extensiones básicas. Los atributos de lo que se compone un certificado se muestran en la siguiente lista:

* Certificado
* Versión
* Número de serie
* Algoritmo usado para firmar el certificado
* Emisor
* Periodo de validez
  + No antes de
  + No después de
* Sujeto
* Información de la clave pública del sujeto
  + Clave pública
  + Algoritmo de la clave pública
* Identificador único del emisor (opcional)
* Identificador único del sujeto (opcional)
* Extensiones (opcional)
* Firma del certificado
* Algoritmo usado para firmar el certificado

Todas las propiedades de los certificados son importantes, pero cabe resaltar las siguientes:

* El número de serie es un número entero mayor de cero y debe ser único para cada certificado emitido por una determinada CA.
* Emisor: es el nombre de la CA que firma el certificado
* Sujeto: a quién va dirigido el certificado. Por ejemplo, en certificados de usuario puede ser el nombre de la persona o en el caso de un certificado para un servidor web, puede ser la URL de un servicio web.

### Extensiones

Las extensiones en los certificados permiten añadir propiedades extra a los certificados. Estas extensiones pueden estar definidas de manera pública y ser usadas por cualquier sistema, pero también se permite la inclusión de extensiones privadas de manera que solo tienen sentido en el sistema que las define.

Dentro de un certificado una extensión está compuesta de:

* Un identificador único de extensión expresado como un OID (Object Identifier). Este OID se expresa en notación ASN.1 de X.690. En el estándar X.690 [8] se definen una serie de formatos de codificación como BER, CER y DER partes de la notación ASN.1. En este caso, cada OID representa casi todos los tipos de objetos posibles que se pueden incluir en un certificado X.509.
* Una estructura ASN.1 que se corresponde al valor de la extensión.

Una extensión sólo puede incluirse una única vez en un certificado.

Cada extensión se puede acompañar de una indicación para informar de la criticidad de la extensión:

* Extensión crítica: si el sistema que usa un certificado encuentra una extensión crítica que no reconoce o no reconoce la información contenida en la extensión debe rechazar el certificado.
* No crítica: el sistema podría ignorar una extensión no crítica si no la reconoce, pero debe procesarla si la reconoce.

Existe un conjunto de extensiones básicas que todo sistema debe reconocer. Estas extensiones permiten el funcionamiento básico de un sistema PKI, por ejemplo, identificando el uso autorizado del certificado o dónde se puede encontrar la información para comprobar la revocación del certificado. En la siguiente lista se nombran algunas de estas extensiones, con un nombre y su identificador OID en formato ASN.1:

* Basic constraints, { id-ce 19 }: indica que el certificado corresponde a una CA, una CA intermedia o si está al final de la cadena.
* Key Usage, { id-ce 15 }: indica el uso permitido del certificado, por ejemplo, cifrado o firma.
* Extended Key Usage, { id-ce 37 }: indica el propósito del certificado, mediante una lista de OID. Estos propósitos podrían ser: ser usado en una conexión TLS, enviar correo electrónico seguro o identificar a una persona.
* Certificate Policies, { id-ce 32 }: refleja las normas que se han seguido para expedir el certificado y los usos de este.
* Para indicar los puntos de acceso para la comprobación de la revocación del certificado (CRL u OCSP), existen dos extensiones:

CRL Distribution Point, { id-ce 31 }

Authority Information Access, { id-pe 1 }

* Subject Alternative Names, { id-ce 17 }: permite asociar el certificado a una lista de sujetos. Complementa la propiedad Sujeto del certificado, permitiendo que sea válido para más nombres. Una organización, por motivos de coste o técnicos, puede optar por un certificado SAN para publicar una web. Es un caso muy común que un certificado para servicios web tenga la extensión SAN para que acceder a una página web con www y sin ella. Por ejemplo, en la siguiente figura, un usuario puede acceder a <https://www.itu.int> o a <https://itu.int> con el mismo certificado:

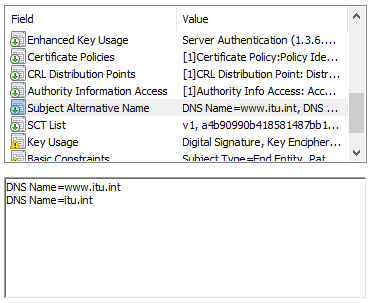


Figura 5. Ejemplo de extensión SAN en el certificado de www.itu.int.

### Formatos de archivo para certificados y PKI

Los formatos de archivo más comunes para almacenar certificados X.509 son los siguientes:

* Formato binario DER. Las extensiones más comunes son: cer, crt, der.
* Privacy-enhanced Electronic Mail. Consiste en un certificado codificado usando la notación DER y posteriormente codificado como Base64 y rodeado por una cabecera y un pie en texto plano. La extensión más común es pem, aunque también es común usar cer o crt.

-----BEGIN CERTIFICATE-----

MIIGOTCCBSGgAwI…

-----END CERTIFICATE-----

* En una estructura PKCS #7, sin datos y usada únicamente para distribuir certificados o CRL. La extensión suele ser p7b o p7c.
* En una estructura PKCS #12, incluyendo claves privadas y certificados, usualmente protegidos con una contraseña. La extensión suele ser p12.
* Usando PFX, el predecesor de PKCS #12, la extensión es pfx. Es también posible encontrar certificados PKCS #12 usando la extensión pfx. El caso habitual es aquellos certificados y claves privadas exportadas desde los sistemas operativos Windows usando su CryptoAPI.

## Cadenas de certificados

En el RFC 3280 se define el concepto de camino de certificados, equivalente al concepto de cadena de certificados. Cuando un usuario usa un servicio que usa un certificado digital, generalmente requiere comprobar la validez de dicho certificado. Para comprobar la validez de un certificado se debe construir la cadena de certificados desde el del servicio hasta el certificado raíz que firma el certificado del servicio.

Para construir la cadena de certificados se inspecciona el emisor del certificado y se compara con el valor del sujeto del propio certificado. Si el emisor es diferente del sujeto, entonces existe un certificado superior en la jerarquía que lo ha firmado. Se realiza esta misma comprobación por cada certificado superior que se descubra hasta que se llegue a un certificado autofirmado, es decir, aquel en el que el sujeto y el emisor sea el mismo. Cuando se llegue a un certificado así, habremos llegado al certificado raíz.

Para que un sistema confíe en un certificado final debe confiar en el certificado raíz que está al final de la cadena de certificados.

Una cadena de certificados tiene las siguientes propiedades:

* La cadena de certificados empieza con el certificado final, le siguen aquellos certificados de CA intermedias y termina con un certificado de una CA raíz. El certificado raíz generalmente será un certificado de una de las CA comerciales o gubernamentales si el certificado es usado públicamente, aunque también puede ser un certificado de una CA no pública como una CA interna de una organización.

Un ejemplo de cadena de certificados en formato pem.

-----BEGIN CERTIFICATE-----

Certificado final

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

Certificado intermedio

-----END CERTIFICATE-----

[...]

-----BEGIN CERTIFICATE-----

Certificado intermedio

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

Certificado raíz

-----END CERTIFICATE-----

* El campo Emisor de un certificado coincide con el campo Sujeto del siguiente certificado de la lista.
* Cada certificado está firmado por la clave privada del siguiente certificado. Evidentemente el último certificado estará firmado por sí mismo para que la cadena pueda terminar.

En las siguientes capturas podemos ver la cadena de certificados para el certificado de [www.itu.int](http://www.itu.int):

COMODO SECURE" 
COMODO RSA Extended Validation Secure Server CA 

Figura 6. Cadena de certificados para www.itu.int.

Machine generated alternative text:
Certificate Info rmation 
This certificate is intended for the following purpose(s): 
• Ensures the identty of a remote computer 
• Proves your identty to a remote computer 
•1.3.6.1.4.1.6449.1.2.1.5.1 
*Refer to the certficabon authority's statement for details. 
vvwvv.itu.nt 
Issued by: COMODO RSA Extended Valida bon Secure Server 
Valid from 28-Mar-17 to 29-Mar-19 
Issuer Statement 

Figura 7. El certificado final está firmado por un certificado intermedio COMODO RSA Extended Validation.

Machine generated alternative text:
Certificate Info rmation 
This certificate is intended for the following purpose(s): 
• Ensures the identty of a remote computer 
• Proves your identty to a remote computer 
• Protects e-mail messages 
• Ensures software came from softvvare publisher 
• Protects software from alteraton after publication 
• Allows data to be signed with the current tme 
*Refer to the certfcaton authority's statement for details. 
Issued to: COMODO RSA Extended Valida bon Secure Server 
Issued by: COMODO RSA Cert ficabon Authority 
Valid from 12-Feb-12 to 12-Feb-27 
Issuer Statement 

Figura 8. El certificado intermedio está firmado por COMODO RSA Certification Authority.

Machine generated alternative text:
Certificate Info rmation 
This certificate is intended for the following purpose(s): 
• Ensures the identty of a remote computer 
• Proves your identty to a remote computer 
• Protects e-mail messages 
• Ensures software came from softvvare publisher 
• Protects software from alteraton after publication 
• Allows data to be signed with the current tme 
Issued to: COMODO RSA Cert fica bon Authority 
Issued by: COMODO RSA Cert ficabon Authority 
Valid from 19-Jan-IO to 19-Jan-38 

Figura 9. COMODO RSA Certification Authority es un certificado raíz ya que es autofirmado.

### Comprobación de la validez de un certificado

Una vez se tiene la cadena de certificados es posible realizar una serie de comprobaciones para determinar si el certificado final que se presente es digno de confianza [9].

Una visión de alto nivel del algoritmo usado para comprobar la validez de la cadena es la siguiente:

1. Empezando por el certificado final, por cada certificado se comprueba:
   1. Que el momento en el que se hace la comprobación está dentro del periodo de validez del certificado.
   2. Se localiza el Emisor del certificado, bien sea porque es el siguiente en la cadena o porque está en la base de datos local de certificados.
   3. Se comprueba la firma del certificado actual con la clave pública del certificado del Emisor obtenido en el punto anterior.
   4. Si el certificado del Emisor venía de la base de datos local de certificados, entonces el proceso termina aquí. En otro caso, se vuelve a empezar el proceso comprobando ahora el certificado Emisor del actual.
2. Además, es posible comprobar la validez del certificado en base a las normas asociadas con cada certificado o con el proceso de validación.
3. Finalmente, también se suele comprobar el estado de la revocación del certificado.

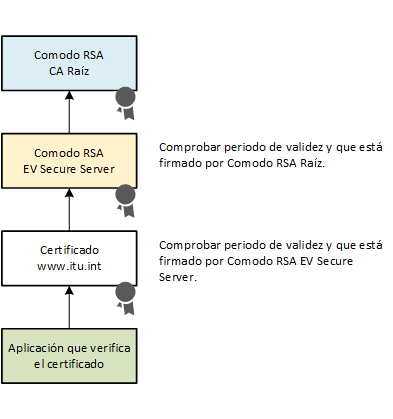


Figura 10. Ejemplo de validación de una cadena de certificados.

Como hemos visto, la comprobación termina cuando en la cadena nos encontramos con un certificado en el que ya confiemos. Es decir, no siempre es necesario llegar hasta el certificado raíz para comprobar la validez de un certificado final. En el ejemplo de la figura 10, si en nuestra base de datos de certificados de confianza nos encontramos con el certificado *Comodo RSA EV Secure Server*, entonces no hace falta que comprobemos este certificado ni el certificado raíz *Comodo RSA CA*.

Una restricción de la comprobación es que un certificado no puede aparecer más de una vez en la cadena. Es decir, no se permiten ciclos en la cadena.

### Certificados autofirmados

Un certificado autofirmado es aquél que está firmado con la clave privada asociada a la clave pública del certificado. Por tanto, en estos certificados el emisor es el mismo que el sujeto. Los certificados raíz, por tanto, deben ser certificados autofirmados, ya que no hay ninguna CA por encima que pueda firmar su certificado.

Debido a la rapidez y facilidad con la que pueden ser emitidos ya que no precisa de ningún proceso de validación por parte de un tercero, estos certificados se suelen usar en entornos de desarrollo de software donde se requiera del uso de un certificado.

## Validación cruzada de certificados

Hay que tener en cuenta que es técnicamente posible tener la misma clave pública firmada por dos CA diferentes y por tanto tener dos certificados para la misma clave pública. En cambio, no es posible tener un único certificado X.509 firmado por más de una CA.

La posibilidad de tener varios certificados por clave pública permite la creación de varias cadenas de certificados para un único certificado ya que se podría construir una cadena por cada certificado raíz.

Gracias a esto es posible, por ejemplo, que un certificado emitido dentro de una PKI pueda ser validado en otra PKI separada y viceversa. La importancia radica en que en cada PKI cada cliente pueda construir la cadena del certificado externo hasta una CA raíz propia de la PKI. En la siguiente figura[[10]](#footnote-11) cada estructura PKI tiene un certificado raíz que está autofirmado y también otro firmado por la CA de la otra estructura PKI. De esta manera es posible construir dos cadenas de certificados para cada certificado de usuario y así, un usuario de PKI 1 puede construir una cadena de certificados para el certificado de Usuario 2 que acabe en el certificado raíz de su estructura PKI.

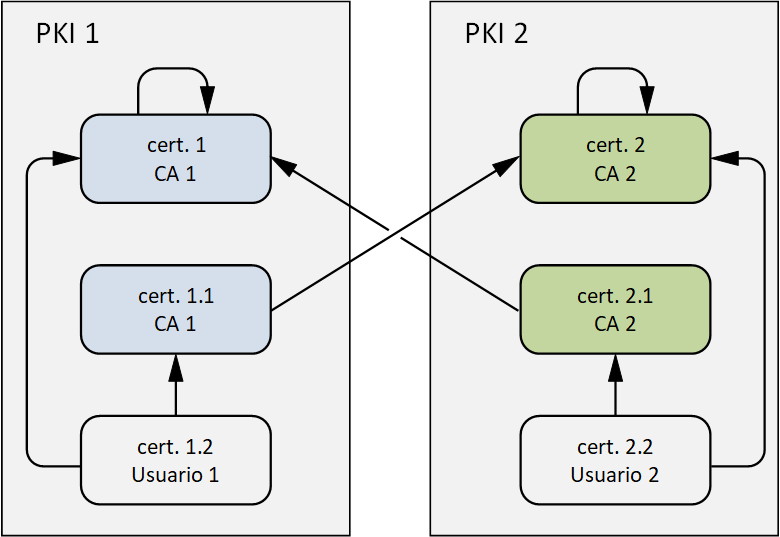


Figura 11. Validación cruzada entre PKI 1 y PKI 2.

La validación cruzada también permite a una CA crear un nuevo certificado raíz sin que los certificados emitidos con el certificado antiguo pierdan su validez. El proceso para generar los nuevos certificados raíz se explica en [10].

## Comprobación de la revocación de un certificado

Cuando se emite un certificado se espera que vaya a ser usado durante todo su periodo de validez. Sin embargo, es posible que un certificado deje de ser usado antes de que expire. Por ejemplo, se ha de cambiar el nombre asociado al certificado, se compromete la clave privada o se termina la relación entre el sujeto y la CA que emitió el certificado. En estos casos, la CA debe revocar el certificado para que no pueda continuar siendo válido.

### Listas de revocación de certificados – CRL

X.509 define un método para revocar certificados que consiste en que cada CA publique periódicamente una lista de revocación de certificados o CRL por sus siglas en inglés Certificate Revocation List. Esta lista consiste en una estructura firmada por la CA o por la entidad que publica la CRL y relaciona una fecha con un certificado que ha sido revocado mediante su número de serie. Por supuesto, estas listas deben ser de dominio público. Lo más normal es que además se distribuyan mediante canales no seguros para que no haya problemas a la hora de negociar la seguridad de la conexión y así poder estar seguros de que un cliente que la solicite pueda descargar la lista sin problemas.

Cuando se ha de comprobar la validez de un certificado, lo normal es obtener una copia más o menos reciente de la CRL de la CA que emitió el certificado y entonces comprobar si el certificado ha sido revocado.

Los certificados que incluyen la extensión CRL Distribution Point incluyen un URI que indica dónde conseguir dicha CRL. Esta URI puede ser una dirección URL a la que se accede por HTTP, una ruta LDAP o incluso una carpeta compartida. Qué tipo de URI se use dependerá del tipo de certificado y, sobre todo, del contexto del uso del certificado. Por ejemplo, un certificado que se use en un sitio web público incluirá una URL a un recurso HTTP. Un certificado que se use únicamente dentro de la red interna de una organización puede incluir una ruta LDAP que apunte a un directorio dentro de dicha organización.

Una limitación del uso de CRL es el tiempo que se tarda en publicar una nueva CRL ya que podría llegar a haber un tiempo considerable entre que un certificado es revocado y la actualización de la CRL de la CA correspondientes.

El formato de la estructura que describe una CRL es el siguiente:

* Algoritmo usado para firmar la CRL
* Firma de la CRL
* CRL
  + Versión (opcional, pero obligatorio con valor entero igual a 1 si se van a usar extensiones)
  + Algoritmo usado para firmar la CRL
  + Emisor (quién emite y firma la CRL)
  + Fecha de emisión
  + Fecha de la siguiente emisión
  + Lista de certificados revocados, por cada certificado
    - Número de serie del certificado
    - Fecha de revocación
    - Extensiones de la entrada
* Extensiones de la CRL

Algunas de las extensiones posibles son para una CRL son:

* Identificador de la clave de la autoridad
* Nombre alternativo del emisor
* Número de CRL

Algunas extensiones posibles de una entrada de certificado son:

* Código de razón de la revocación
* Fecha desde la que se sospecha que el certificado ha sido comprometido

|  |  |
| --- | --- |
|  |  |

Figura 12. CRL de Starfield Secure Certificate Authority - G2. Detalles y certificados revocados.

### Online Certificate Status Protocol – OCSP

Online Certificate Status Protocol es un protocolo usado para obtener el estado de la revocación de un certificado X.509. Se describe en el RFC 6960 [11]. Es una alternativa al uso de CRL y surgió para aliviar algunos de los problemas típicos de CRL. A un servidor OCSP se le conoce como "OCSP Responder".

La comunicación entre un cliente y un servidor OCSP se realiza mediante el protocolo HTTP usando mensajes codificados en ASN.1. Una diferencia respecto a las CRL es que la conexión con un servidor OCSP sí puede ser HTTPS y quizá en algunos casos pueda ser conveniente, como cuando se pregunta sobre el estado de certificados de usuario. De cualquier manera, el uso de HTTPS para comunicarse con el servidor OCSP no es obligatorio.

La principal diferencia entre OCSP y CRL es que cuando se solicita una CRL obtenemos una lista completa de todos los certificados revocados por una CA y esta lista puede llegar a ser de un tamaño considerable. En cambio, a un servidor OCSP se le pide el estado de un único certificado y por tanto la respuesta es generalmente más ligera y conlleva un ahorro de ancho de banda y tiempo de proceso por parte del cliente.

Sin embargo, el uso del protocolo OCSP implica que el propietario de la CA debe tener disponible permanentemente online el servicio para que un sistema pueda contactarlo. Además, este debe responder en el menor tiempo posible para que no provoque lentitud por los tiempos de respuesta en el sistema que comprueba un certificado.

Al igual que con CRL una CA incluye una extensión Authority Information Access en sus certificados donde indica la URL del servidor OCSP que conoce el estado de revocación de los certificados emitidos por la CA.

El protocolo OCSP tiene un funcionamiento en modo pregunta/respuesta:

1. El sistema que comprueba el estado de un certificado pregunta al servidor OCSP asociado al certificado por el estado de este. En la pregunta le envía el número de serie del certificado.
2. El servidor OCSP usa este número de serie para buscar el estado del certificado en la base de datos de la CA. Cuando conoce el estado del certificado, envía una respuesta firmada al usuario indicando el estado del certificado.
3. El usuario comprueba la firma de la respuesta usando la clave pública de la CA que firmó el certificado sobre el que se preguntaba.

Una respuesta consiste en:

* Campos como versión, algoritmo de firma y valor de la firma.
* Identificador del servidor que responde.
* Duración de la validez de la respuesta.
* Respuestas por cada uno de los certificados de la petición.
* Extensiones.

Los posibles valores de la respuesta son:

* El certificado es válido.
* El certificado está revocado.
* No se conoce el estado del certificado.
* Además, también se incluye la duración de la respuesta por cada certificado.

Finalmente, para que un cliente pueda considerar la respuesta como válida debe ser firmada por una de las tres siguientes entidades:

* La CA que emitió el certificado sobre el que se pregunta.
* Un Responder de confianza del usuario que pregunta.
* Un Responder autorizado por la CA. Este Responder tendrá un certificado firmado directamente por la CA emisora que le identificará como Responder autorizado para dar respuestas OCSP para esta CA.

### OCSP Stapling

Para mitigar el principal problema de rendimiento de OCSP, donde un Sistema debe contactar con el respondedor OCSP cada vez que se encuentra un certificado, se definió la extensión Certificate Stauts Request para el protocolo TLS en el RFC 6066 [12].

Esta extensión permite al cliente de una conexión TLS solicitar al servidor el estado de la revocación del certificado. Si el servidor entiende la petición, enviará una respuesta OCSP durante la negociación del protocolo TLS. Por supuesto, para que el cliente pueda aceptar dicha respuesta OCSP, esta tiene haber estado originada en el servidor OCSP original ya que debe estar firmada por la misma CA que firma el certificado del servidor. Por tanto, para que el servidor pueda devolver esta respuesta al cliente, debe haber contactado previamente con el servidor OCSP y haber almacenado dicha respuesta temporalmente. Es esta misma respuesta la que enviará al cliente cuando se la soliciten.

El tiempo que el servidor puede almacenar la respuesta OCSP original depende precisamente del tiempo que dicha respuesta sea válida y está determinado las mismas propiedades de la respuesta.

Cuando un cliente recibe una respuesta debe comprobar su validez y, si no es aceptada, entonces parar la conexión. Si no recibiera una respuesta entonces contactaría directamente con el servidor OCSP.

El problema de que el servidor mantenga en una caché las respuestas OCSP es que esto introduce un retraso en la revocación efectiva de un certificado ya que puede pasar una cantidad de tiempo indeterminada desde que un certificado es revocado hasta que la última respuesta OCSP cacheada expira.

Aun así, esta extensión al protocolo TLS optimiza el establecimiento de una conexión ya que evita que el cliente tenga que contactar al servidor OCSP y obtiene esa respuesta directamente desde el servidor con el que ya tiene una conexión. De esta manera, en el cliente se evitan varias conexiones (DNS para resolver el nombre del servidor OCSP y la petición HTTP hacia el mismo) y también se reduce el número de peticiones que se hacen al servidor OCSP en general.

La especificación de esta extensión solo permite que se envíe una única respuesta OCSP por conexión, por lo que en general es insuficiente para comprobar la validación de un certificado. Al solo tener una respuesta OCSP posible, que será para el certificado del servidor, esto impide poder comprobar por esta vía la validez del certificado raíz o intermedios que pudieran existir en la cadena de certificados. Para solucionar este problema se especifica la extensión TLS Multiple Certificate Status Request Extension [13] que ya permite solicitar y enviar respuestas OCSP para todos los certificados de la cadena.

## Autoridades de certificación

Una autoridad de certificación es la entidad que se encarga de generar certificados a partir de las claves públicas que recibe. De esta manera, es la autoridad certificadora la que garantiza que la clave pública que está firmando pertenece al sujeto del certificado.

Por tanto, una CA es una pieza clave en una estructura PKI jerárquica ya que, en el árbol que se podría representar en dicha estructura, es todos y cada uno de los nodos que no son hojas (certificados finales).

El certificado que usa una CA suele tener:

* Key Usage: Certificate Signing
* Basic Constraints: Subject Type=CA

Adicionalmente, podría tener más valores en las propiedades Key Usage, Key Enhanced Usage o Basic Constraints. Por ejemplo, para firmar una CRL el valor de Key Usage debe ser Off-line CRL Signing o para firmar una respuesta OCSP el valor de Key Enhanced Usage debe ser OCSP Signing.

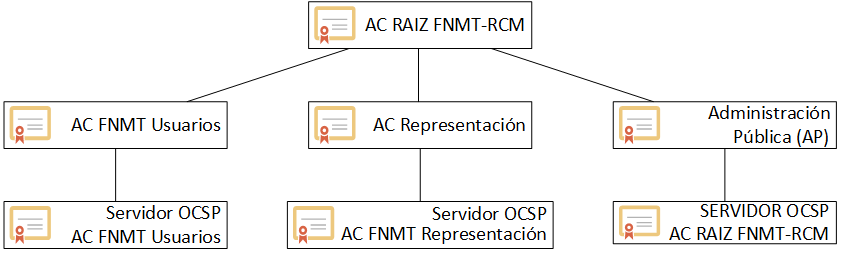


Figura 13. Esquema parcial de la jerarquía de certificados CA de la Fábrica Nacional de Moneda y Timbre (FNMT).

### Proceso de emisión de un certificado

Cuando una entidad quiere solicitar un certificado a una autoridad de certificación, la autoridad elegida recibe una solicitud de firma de certificado llamada CSR (Certificate Signing Request).

El procedimiento habitual para solicitar un certificado es:

1. Generar una pareja de claves por parte del sistema que solicitará el certificado.
2. Se recogen una serie de datos extras a enviar a la autoridad como pueden ser:
   * El DN o CN que se quiere relacionar con el certificado.
   * Información sobre la empresa, departamento, geográfica, etc.
   * Una dirección de correo electrónico.
   * Además, dependiendo del tipo de certificado que se esté solicitando las CA suelen requerir otro tipo de información, ya sea de manera telemática o física.
3. Se envía el CSR a la autoridad de certificación.
4. Por lo general, la autoridad hará algún tipo de validación de la información, sobre todo confirmará la identidad del solicitante con relación al certificado que se haya pedido, por ejemplo:
   * Para un certificado de usuario, por ejemplo, un certificado de usuario de la FNMT, el solicitante suele tener que ir a una de las oficinas de Hacienda o de otro organismo del gobierno con la solicitud y su DNI para que el funcionario de turno haga la comprobación de que el solicitante es el mismo que la persona que se nombre en el CSR[[11]](#footnote-12).
   * Para un certificado para un nombre DNS, por ejemplo, para poder conectarnos a una web usando HTTPS, la autoridad suele confirmar que el solicitante es administrador o propietario del dominio, con frecuencia enviando un correo electrónico a una lista limitada de direcciones reservadas habituales, por ejemplo: hostmaster, webmaster, etc. Otro método habitual es crear un registro TXT en el servidor DNS con un valor indicado por la CA. De esta manera, se
   * Existen también otros procesos más complejos. Las autoridades comerciales suelen tener clases de certificados de validación extendida que, en los navegadores modernos, hacen que la barra de direcciones cambia a otro color, para indicar de una manera más llamativa que se está usando una conexión cifrada. Por lo general, es necesario justificar la expedición de estos certificados demostrando el capital de la empresa solicitante, mediante justificantes de impuestos, contacto físico con el administrador/responsable de la empresa o procedimientos similares.
5. Una vez que la identidad del solicitante se haya validado, la autoridad procede a emitir el certificado solicitado.

A la hora de solicitar certificados, existen otras autoridades que pueden entrar en juego:

* VA, Validation Authority. Este ente se encargaría de pedir y validar los datos identificativos de la persona que está solicitando el certificado.
* RA, Registration Authority. Este ente se encargaría de aprobar que la persona que solicita el certificado está autorizada para solicitar un certificado en nombre del Sujeto del certificado.

### Tipos de CSR

Independientemente del formato de una solicitud CSR, esta debe incluir una serie de datos mínimos para que una CA pueda generar un certificado a partir de ella. Obviamente, debe incluir la clave pública del sujeto, el sujeto y el uso que se quiere hacer de dicho certificado. Respecto a los formatos de CSR, los más habituales son PCKS #10 y SPKAC.

Cabe decir que una CA es libre de usar los atributos que se envían en la CSR o no. Es común que una CA necesite un CSR únicamente para recibir la clave pública en un formato determinado y que ignore el resto de los atributos en el CSR. Será ella misma la que determine el valor del resto de atributos del certificado.

#### PKCS #10

El formato PKCS #10 [14] es el más usado habitualmente. El formato de una CSR PCKS #10 se compone de tres partes:

1. Información de la solicitud. Esta solicitud está formada por:
   * El DN (nombre distinguido) de la entidad que realiza la solicitud.
   * La clave pública.
   * Otros atributos sobre sobre la solicitud o sobre el sujeto. Aquí se pueden usar atributos definidos en PKCS #9 [15] para extender el certificado que se solicita.
2. El algoritmo de firma usado para firmar la información de la solicitud.
3. El valor de la firma de la solicitud.

#### SPKAC

Signed Public Key and Challenge o SPACK, también conocido como Netscape SPKI.

Este formato de CSR que se manipula con OpenSSL y que es el que implementan los navegadores web compatibles con Mozilla en el elemento keygen. Este elemento forma parte de la especificación HTML5, pero su uso está desaconsejado actualmente ya que los navegadores que lo soportan actualmente tienen planes de quitar su soporte y la última especificación de HTML 5.2 ha quitado el elemento[[12]](#footnote-13). No está soportado por Internet Explorer.

Esta implementación se usa dentro de formularios en páginas web para generar parejas de claves y enviar un CSR a un servidor web (almacenando el navegador la clave privada). El servidor que recibe la solicitud hará las comprobaciones pertinentes y creará un certificado que enviará al navegador. Estos certificados suelen ser por tanto certificados de usuario que después podrá usar el navegador para autenticarse con un sitio web mediante HTTPS.

Dado que es un formato que se envía mediante un formulario web, es un formato en texto plano con una serie de variables en formato Clave=Valor como, por ejemplo[[13]](#footnote-14):

|  |
| --- |
| SPKAC=MIIBXjCByDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA3L0IfUijj7+A8CPC8EmhcdNoe5fUAog7OrBdhn7EkxFButUp40P7+LiYiygYG1TmoI/a5EgsLU3s9twEz3hmgY9mYIqb/rb+SF8qlD/K6KVyUORC7Wlz1Df4L8O3DuRGzx6/+3jIW6cPBpfgH1sVuYS1vDBsP/gMMIxwTsKJ4P0CAwEAARYkYzBkZjFlYjctMTU0NC00MWVkLWFmN2EtZDRkYjBkNDc5ZjZmMA0GCSqGSIb3DQEBBAUAA4GBALEiapUjaIPs5uEdvCP0gFK2qofo+4GpeK1A43mu28lirYPAvCWsmYvKIZIT9TxvzmQIxAfxobf70aSNlSm6MJJKmvurAK+Bpn6ZUKQZ6A1m927LvctVSYJuUi+WVmr0fGE/OfdQ+BqSm/eQ3jnm3fBPVx1uwLPgjC5g4EvGMh8M  CN=Joe Snuffy  OU=Snake Oil, LLC  O=Department of pricing  L=City name  ST=State or province  C=United States  E=joe.snuffy@snakeoil.com |

Ejemplo de SPKAC que incluye la clave pública y el DN del solicitante

Siendo SPKAC la variable crítica dado que es ahí donde se incluye la clave pública. También incluye una frase de paso, contraseña o reto que es enviada por el servidor. Esta contraseña debería ser generada aleatoriamente por el servidor y enviada en cada petición para así impedir que un CSR SPKAC pueda ser reutilizado por un atacante[[14]](#footnote-15).

### Distribución del certificado generado

Dependiendo del tipo de certificado solicitado, la CA distribuirá el certificado de diferente manera:

* Para certificados de usuario o los usados en servidores web o de correo, se suelen descargar de la página web de la CA donde se ha comprado el certificado. También es posible que la CA muestre el certificado en texto plano, codificado en Base64 para que el solicitante lo copie y guarde localmente en su máquina.

Este procedimiento podría parecer inseguro, pero hay que tener en cuenta que para poder usar el certificado descargado es necesario tener la clave privada y esta no se ha transmitido en ningún momento por la red.

* También es posible que el certificado se transmita físicamente a la memoria de una smart card u otro dispositivo físico como un Trusted Platform Module (TPM). Parece lógico pensar entonces que cuando se emite un certificado de este tipo, el solicitante debe desplazarse físicamente a la entidad que lo haya expedido. Un ejemplo de esto es el DNIe. Cuando el certificado de usuario que lleva incorporado el DNIe expira, el ciudadano debe ir a una comisaría de Policía donde debe ir a una máquina que escribirá el certificado renovado en el chip de su DNIe.

### Seguridad relacionada con una CA

Como se puede suponer, si se compromete la clave privada de una CA, todos los certificados que hayan sido firmados por esa clave, deberían dejar de ser válidos, incluidos los certificados de otras CA que esta clave haya firmado. Esto es porque ya no se puede confiar en los certificados que se emitan desde el momento en el que se sepa que la CA ha sido comprometida. El poseedor de la clave privada comprometida podría generar tantos certificados como quisiera haciéndose pasar por la CA.

Por este motivo los certificados de una CA raíz se suelen mantener en secreto y offline y se suele confiar en una CA subordinada para generar certificados para entidades finales.

## Confianza en una PKI

¿Podemos realmente confiar en los certificados raíz o intermedios que vienen incluidos en los navegadores web o en los sistemas operativos?

El usuario normal "confía" ciegamente en las CA que su sistema operativo o navegador trae instaladas y no se preocupa por el proceso de comprobar la validez de los certificados. Evidentemente, la gran mayoría de los usuarios desconoce el sistema PKI o ni siquiera sabe que lo está usando por lo que este proceso de confianza se obvia en la mayoría de los casos.

Aunque aún queda mucha educación de cara a los usuarios, se les ha enseñado que están protegidos cuando en su navegador web se ve el icono de un candado y entonces el usuario ya se siente seguro sin sentir la necesidad de ninguna otra comprobación. Por su parte, los navegadores suelen mostrar páginas de error o mensajes bastante llamativos cuando el usuario quiere entrar en una página web mediante HTTPS y el certificado del servidor tiene algún problema de validación.

Los certificados que normalmente están instalados por el sistema operativo son certificados raíz y certificados intermedios, pero ¿qué impide a una CA firmada por uno de estos certificados raíz u otra CA subordinada de estas generar un certificado para un nombre que ya existe y realizar un ataque tipo man-in-the-middle? Obviamente hace falta comprometer más dispositivos que un certificado para poder realizar un ataque MITM, pero la posibilidad existe. Una organización podría hacer uso de un certificado de CA para realizar una monitorización de las conexiones cifradas dentro de la empresa si instalara un dispositivo de red a modo de proxy que intervenga las conexiones HTTPS y que pudiera generar al vuelo certificados para los nombres de servicios a los que sus empleados quieran entrar. Existen mecanismos para confirmar la identidad del servidor, pero un usuario medio no va a saber ni siquiera que el MITM está ocurriendo. Para el caso de una CA raíz pública, muchas de estas siguen las pautas establecidas en *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*[[15]](#footnote-16). Estas pautas indican qué tipo de políticas y normas son aceptables para las entidades que disponen de una CA pública.

Por otra parte, ¿podemos estar seguros de que nadie puede usar nuestra clave privada? Normalmente, un usuario guardará su clave privada en su máquina y puede que esté comprometiendo su clave al hacerlo así. Un virus o software malicioso podría estar usando la clave sin que el usuario lo sepa. Por otra parte, incluso si la clave está protegida por una contraseña, ¿cómo de segura es esta contraseña? Si el certificado se almacenara en una Smart-Card o TPM usando un código de acceso PIN estamos ante la misma pregunta. Si no podemos estar seguros de que nadie más está teniendo acceso a nuestra clave privada, ¿realmente se puede garantizar la seguridad en la autenticación que proporciona el sistema?

Confiamos en que el sujeto del certificado es el mismo que el que nos presenta el certificado, pero ¿podemos estar seguros de que son la misma persona? ¿Cómo podemos saber que no ha sido otra persona la que ha solicitado el certificado haciéndose pasar por el sujeto del certificado? Es cierto que muchas CA comerciales usan el sistema de Validación Extendida, pero un usuario no tiene por qué saber qué es eso ni cómo funciona y una organización puede no querer gastar ese dinero extra en obtener un certificado de este tipo. Por esto es tan importante el método de validación de la identidad del solicitante de cara a emitir un certificado.

Finalmente, ¿qué pasa si se nos presenta un certificado que no usa CRL u OCSP? Dependemos completamente de la implementación de PKI del software que estemos usando para que nos advierta de tal problema. Incluso si se usa CRL/OCSP, es posible desactivar esta comprobación en muchas aplicaciones por lo que estamos perdiendo un gran grado de seguridad.

Como vemos, el sistema PKI se basa en la confianza ciega en el propio sistema y en que las CA van a hacer bien su trabajo. Bien implementada y desplegada es un sistema seguro, pero seguimos siendo personas y se pueden cometer errores.

# Requisitos del sistema

## Participantes

### Organizaciones participantes

|  |  |
| --- | --- |
| **Organización** | **Universidad de Sevilla** |
| **Dirección** | ETSII Informática |
| **Teléfono** | **PD** |
| **Fax** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Organización** | **WebCA** |
| **Dirección** | **PD** |
| **Teléfono** | **PD** |
| **Fax** | **PD** |
| **Comentarios** | Ninguno |

### Personas participantes

|  |  |
| --- | --- |
| **Participante** | **Jesús Fernández** |
| **Organización** | [WebCA](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ORG-0002) |
| **Rol** | Alumno |
| **Es desarrollador** | Sí |
| **Es cliente** | No |
| **Es usuario** | No |
| **Comentarios** | Ninguno |

## Objetivos del sistema

|  |  |
| --- | --- |
| **OBJ-0001** | **Emitir certificados digitales** |
| **Versión** | 1.0 (11/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | El sistema deberá poder emitir certificados digitales en base a una solicitud de un usuario |
| **Subobjetivos** | Ninguno |
| **Importancia** | vital |
| **Urgencia** | inmediatamente |
| **Estado** | en construcción |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0002** | **Revocar certificados digitales** |
| **Versión** | 1.0 (11/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | El sistema deberá llevar un seguimiento de qué certificados digitales ha emitido y cuáles de ellos son válidos o han sido revocados |
| **Subobjetivos** | Ninguno |
| **Importancia** | vital |
| **Urgencia** | inmediatamente |
| **Estado** | en construcción |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0008** | **Administrar plantillas de certificados** |
| **Versión** | 1.0 (16/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | El sistema deberá ser capaz de poder ofrecer a los usuarios diferentes plantillas de certificados digitales para los que pueden solicitar un certificado digital. Cada plantilla debe definir una serie de parámetros para los certificados expedidos siguiendo la misma, así como una serie de requisitos que los usuarios deben cumplir para poder solicitar un certificado con una determinada plantilla |
| **Subobjetivos** | Ninguno |
| **Importancia** | importante |
| **Urgencia** | hay presión |
| **Estado** | en construcción |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0009** | **Llevar un registro de los usuarios del sistema** |
| **Versión** | 1.0 (19/02/2018) |
| **Autores** | **?** |
| **Fuentes** | **?** |
| **Descripción** | El sistema deberá **PD** |
| **Subobjetivos** | Ninguno |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0010** | **Registro de validez de los certificados emitidos** |
| **Versión** | 1.0 (19/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | **?** |
| **Descripción** | El sistema deberá **PD** |
| **Subobjetivos** | Ninguno |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0011** | **Realizar validaciones previas a la emisión de un certificado** |
| **Versión** | 1.0 (02/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | El sistema deberá llevar a cabo algún tipo de validación previa a la emisión de un certificado para tener una seguridad mínima que el solicitante del certificado tiene derecho a solicitar el tipo de certificado que quiere |
| **Subobjetivos** | Ninguno |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0012** | **Administrar la autoridad de certificación** |
| **Versión** | 1.0 (13/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | El sistema deberá dar opciones para administrar la autoridad de certificación como cambiar los permisos de los usuarios, cambiar el certificado de la CA o realizar tareas que puedan afectar al servicio que proporciona la autoridad de certificación |
| **Subobjetivos** | Ninguno |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

## Catálogo de requisitos del sistema

### Requisitos de información

Información que debe almacenar el sistema para cumplir los objetivos, indicando datos específicos.

|  |  |  |
| --- | --- | --- |
| **IRQ-0001** | **Usuario** | |
| **Versión** | 1.0 (01/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002)   [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001) | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a un usuario que hace uso del sistema que tendrá una serie de actividades disponibles según el rol que tenga en el sistema. En concreto: | |
| **Datos específicos** | * Identificador (El identificador será la dirección de correo electrónico del usuario) * Clave pública * Nombre * Rol * Eliminado * Motivo eliminación | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0007** | **Rol de usuario** | |
| **Versión** | 1.0 (27/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002) | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a los diferentes roles de los usuarios que participan en las actividades de la autoridad de certificación donde el usuario de cada rol debe satisfacer una serie de restricciones. En concreto: | |
| **Datos específicos** | * Tipo de rol * Restricciones | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0002** | **Certificado emitido** | |
| **Versión** | 1.0 (01/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001) | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a un certificado digital que hay emitido incluyendo el usuario solicitante, la plantilla que se usó para emitir el certificado y el estado de revocación. En concreto: | |
| **Datos específicos** | * Sujeto del certificado * Fecha de inicio de validez * Fecha de fin de validez * Certificado emitido * Usuario solicitante * Identificador de la plantilla * Versión de la plantilla * Estado de revocación * Fecha de la revocación * Motivo de la revocación | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0003** | **Solicitud de certificado** | |
| **Versión** | 1.0 (01/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001) | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a una solicitud de emisión de un certificado digital incluyendo el usuario que hizo la solicitud y la plantilla que se requiere. En concreto: | |
| **Datos específicos** | * CSR * Identificador de la plantilla * Versión de la plantilla * Usuario solicitante * Estado de la solicitud | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0004** | **Plantilla de certificado** | |
| **Versión** | 1.0 (01/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010)   [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011) | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a una plantilla para emitir certificados digitales que define una serie de restricciones sobre las diferentes opciones para emitir certificados y también sobre las extensiones que incluirá el certificado. En concreto: | |
| **Datos específicos** | * Identificador * Versión * Nombre * Restricciones del certificado * Visible * Nombre a mostrar * OID | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Una plantilla se usa para establecer unos valores predeterminados para las diferentes propiedades de un certificado o para restringir el uso del mismo. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **IRQ-0006** | | **Autoridad de Certificación** | |
| **Versión** | | 1.0 (01/02/2018) | |
| **Autores** | | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** | |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002) | |
| **Descripción** | | El sistema deberá almacenar la información correspondiente a una autoridad de certificación que puede emitir certificados digitales. En concreto: | |
| **Datos específicos** | | * Nombre * Pareja de claves * Certificado público | |
| **Tiempo de vida** | | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | | **PD** | |
| **Urgencia** | | **PD** | |
| **Estado** | | **PD** | |
| **Estabilidad** | | **PD** | |
| **Comentarios** | La AC no tiene por qué tener un solo certificado para firmar. Si se decide cambiar el certificado, hay que mantener el antiguo para poder seguir firmando la CRL del mismo. | | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0008** | **Validación** | |
| **Versión** | 1.0 (01/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001) | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a una validación de identidad requerida por una plantilla de certificado. En concreto: | |
| **Datos específicos** | * Tipo de validación * Fecha de expiración * Valor asociado (El valor asociado puede ser, por ejemplo, un nombre de dominio DNS o una dirección de correo electrónico.) * Fecha de expiración | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| **PD** | **PD** |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

### Requisitos de restricción

Regla de negocio que debe tenerse en cuenta al desarrollar el nuevo sistema.

|  |  |  |
| --- | --- | --- |
| **CRQ-0001** | **Emisión solo a usuarios registrados** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001) | |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: solo los usuarios registrados en el sistema pueden solicitar un certificado digital. | |
| **Importancia** | vital | |
| **Urgencia** | inmediatamente | |
| **Estado** | en construcción | |
| **Estabilidad** | **PD** | |
| **Comentarios** | | Ninguno |

|  |  |
| --- | --- |
| **CRQ-0002** | **Correo electrónico autorizado** |
| **Versión** | 1.0 (27/03/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Dependencias** |  [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009) |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: el sistema debe comprobar que el correo electrónico del usuario tiene un dominio autorizado por los operadores de la autoridad de certificación |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |  |
| --- | --- | --- |
| **CRQ-0003** | **Uso de certificados de operadores** | |
| **Versión** | 1.0 (01/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0012] Administrar la autoridad de certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0012) | |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: un certificado de usuario asociado con una cuenta de usuario tipo operador no se puede usar para solicitar certificados digitales | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | | Ninguno |

|  |  |
| --- | --- |
| **CRQ-0004** | **Uso de certificados de usuario final** |
| **Versión** | 1.0 (01/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001) |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: un certificado de usuario final solo se puede usar para solicitar certificados digitales y realizar validaciones de identidades |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **CRQ-0005** | **Validación de identidad necesaria** |
| **Versión** | 1.0 (01/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011) |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: si una plantilla de certificado exige algún tipo de validación de identidad, un usuario solo puede solicitar un certificado para esa plantilla si tiene una validación registrada y validada según la identidad necesaria |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **CRQ-0006** | **Expiración antes que la AC Raíz** |
| **Versión** | 1.0 (01/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010) |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: la fecha de expiración de un certificado generado por la autoridad de certificación no puede ser posterior que la fecha de expiración del certificado aíz del certificado que se use para firmar |
| **Importancia** | quedaría bien |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **CRQ-0007** | **Solicitud de revocación** |
| **Versión** | 1.0 (11/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002) |
| **Descripción** | La información almacenada por el sistema deberá satisfacer la siguiente restricción: Solo un usuario que ha solicitado un certificado puede solicitar su revocación |
| **Importancia** | **PD** |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

### Requisitos funcionales

#### Definición de actores

|  |  |
| --- | --- |
| **ACT-0001** | **Administrador** |
| **Versión** | 1.0 (11/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | Este actor representa un usuario que tiene acceso a todas las partes del sistema, incluyendo la posibilidad de cambiar la pareja de claves y el certificado que usa esta autoridad de certificación para firmar los certificados emitidos. La autenticación de este usuario al sistema será con un certificado digital. |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **ACT-0002** | **Operador** |
| **Versión** | 1.0 (11/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | Este actor representa un usuario que tiene acceso a la parte de administración de la autoridad de certificación donde puede configurar el servicio y controlar la emisión de los certificados si fuera necesario. La autenticación de este usuario al sistema será con un certificado digital. |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **ACT-0003** | **Usuario registrado** |
| **Versión** | 1.0 (11/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | Este actor representa un usuario conocido por el sistema y que puede solicitar la emisión o revocación de certificados digitales firmados por esta autoridad de certificación. La autenticación de este usuario al sistema será con un certificado digital. |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **ACT-0004** | **Usuario anónimo** |
| **Versión** | 1.0 (11/02/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | Este actor representa un usuario desconocido para el sistema por lo que no puede realizar ninguna otra acción que no sea registrarse en el sistema |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **ACT-0005** | **Instalador** |
| **Versión** | 1.0 (13/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) |
| **Descripción** | Este actor representa un usuario que realiza la instalación de la autoridad de certificación y que va a realizar la configuración inicial y crear el primer usuario administrador. Este usuario será un usuario local del sistema operativo donde se instale el software. |
| **Comentarios** | Ninguno |

#### Casos de uso del sistema

* Servicio que el sistema debe prestar a los actores.
* Constan de pasos que pueden tener excepciones.

##### Registro de usuarios

Casos de uso relacionados con el registro y administración de los usuarios que van a partiticipar en esta autoridad de certificación, ya sea como usuario final o como operador.

|  |  |  |
| --- | --- | --- |
| **UC-0001** | **Registro de un usuario anónimo** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0003] Solicitud de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0003)   [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001)   [[CRQ-0002] Correo electrónico autorizado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0002)   [[CRQ-0006] Expiración antes que la AC Raíz](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0006)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario anónimo accede a la aplicación web | |
| **Precondición** | El usuario debe tener una cuenta de correo electrónico pública | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario anónimo (ACT-0004)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0004) accede al sistema iniciando una nueva sesión en el sistema |
| 2 | El sistema ofrece al usuario tres opciones: autenticarse, registrarse o recuperar una cuenta |
| 3 | El actor [Usuario anónimo (ACT-0004)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0004) elige la opción de registrar un nuevo usuario |
| 4 | El sistema solicita al nuevo usuario los datos necesarios para registrar un nuevo usuario, entre ellos, una dirección de correo electrónico |
| 5 | El actor [Usuario anónimo (ACT-0004)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0004) rellena los datos solicitados por el sistema |
| 6 | Se realiza el caso de uso [Validación de correo electrónico (UC-0022)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0022) |
| 7 | El sistema procesa el registro del nuevo usuario y lo pone en la cola de solicitudes de certificado de usuario |
| 8 | Si el sistema está configurado para permitir el registro automático de nuevos usuarios, el sistema autoriza la emisión del certificado de usuario |
| 9 | Si el sistema está configurado para que el registro de nuevos usuarios esté supervisado por un operador, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) revisa la petición de registro de nuevo usuario y, si acepta el registro, autoriza la emisión del certificado de usuario |
| 10 | El sistema procesa la autorización del registro de nuevo usuario, expide el certificado de usuario y envia el certificado al usuario |
| **Postcondición** | El usuario recibe un certificado de usuario que le permite autenticarse en la aplicación web | |
| **Excepciones** | **Paso** | **Acción** |
| 6 | Si la validación del correo electrónico falla, el sistema comunica al usuario el fallo, a continuación este caso de uso queda sin efecto |
| 9 | Si el Operador no acepta el registro del nuevo usuario, el sistema comunica al usuario el motivo del rechazo, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | vital | |
| **Urgencia** | inmediatamente | |
| **Estado** | en construcción | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0002** | **Renovación o reemisión de un certificado de usuario** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002)   [[CRQ-0006] Expiración antes que la AC Raíz](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0006)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario registrado quiera acceder al sistema, pero su certificado de usuario ha expirado o se ha sido perdido | |
| **Precondición** | El usuario debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) accede al sistema iniciando una nueva sesión |
| 2 | El sistema ofrece al usuario tres opciones: autenticarse, registrarse o recuperar una cuenta |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) elige la opción de recuperar una cuenta de usuario |
| 4 | El sistema solicita la dirección de correo electrónico con la que el usuario está registrado en el sistema y envía un código único con el que el usuario puede confirmar que es el propietario de esa dirección de correo electrónico |
| 5 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) recibe el correo electrónico e inserta el código único en el sistema |
| 6 | El sistema recibe el código único, confirma que el código corresponde con una solicitud de renovación, expide un nuevo certificado de usuario y se lo envía al usuario |
| **Postcondición** | El usuario recibe un nuevo certificado de usuario | |
| **Excepciones** | **Paso** | **Acción** |
| 6 | Si el código único no corresponde con una solicitud de renovacion vigente, el sistema comunica el fallo al usuario, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | vital | |
| **Urgencia** | hay presión | |
| **Estado** | en construcción | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0003** | **Cancelación de registro iniciada por usuario** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002)   [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el usuario no desea seguir usando el servicio | |
| **Precondición** | El usuario debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) accede al sistema y se autentica para iniciar una nueva sesión |
| 2 | El sistema muestra la página de bienvenida |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) selecciona la opción de administrar su cuenta o perfil y, entonces, selecciona cancelar su registro |
| 4 | El sistema solicita confirmación al usuario para llevar a cabo la acción, preguntando si el usuario está seguro. Adicionalmente, el sistema puede preguntar al usuario si revocar todos los demás certificados que están asociados con su usuario |
| 5 | Si el usuario accede a cancelar su registro, el sistema revoca todos los certificados de usuario asociados a este usuario |
| 6 | Si el usuario accede a revocar todos los certificados asociados con su usuario, el sistema revoca todos los certificados que hayan sido solicitados por este usuario que aún sean vigentes |
| **Postcondición** | Todos los certificados de usuario del usuario registrado quedan revocados y el usuario deja de poder usar el sistema | |
| **Excepciones** | **Paso** | **Acción** |
| 5 | Si el usuario no confirma la acción, el sistema dejará sin efecto la cancelación del registro, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | vital | |
| **Urgencia** | inmediatamente | |
| **Estado** | en construcción | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0004** | **Cancelación de registro iniciada por administrador** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001)   [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador de la autoridad de certificación inicia la cancelación del registro de un usuario unilateralmente | |
| **Precondición** | El usuario debe estar registrado en la autoridad de certificación | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede al sistema y realiza una búsqueda por el usuario al que se quiere cancelar su registro |
| 2 | El sistema devuelve los detalles del usuario que se busca y le da opciones para administrar el mismo |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la opción de eliminar la cuenta del usuario |
| 4 | El sistema solicita al operador el motivo de la eliminación |
| 5 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) registra el motivo de la eliminación |
| 6 | El sistema marca al usuario como eliminado y revoca los certificados de usuario asociados al usuario |
| 7 | El sistema marca como revocados los certificados que se hubieran emitido al usuario usando como motivo de revocación el que hubiera especificado el operador |
| **Postcondición** | El usuario deja de estar registrado quedando todos sus certificados de usuario revocados | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

##### Validación de identidades

Casos de uso relacionados con los procesos de validación de la identidad del usuario u otras validaciones relacionadas con la emisión de certificados digitales.

|  |  |  |
| --- | --- | --- |
| **UC-0021** | **Validación de un dominio DNS** | |
| **Versión** | 1.0 (30/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0008] Validación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0008)   [[CRQ-0001] Emisión solo a usuarios registrados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0001)   [[CRQ-0005] Validación de identidad necesaria](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0005)   [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario registrado quiera validar que un dominio DNS es de su propiedad para poder solicitar un certificado para ese dominio | |
| **Precondición** | El usuario que solicita la validación debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) accede al sistema y solicita una nueva validación de dominio DNS |
| 2 | El sistema solicita el nombre del dominio DNS que se quiere validar |
| 3 | Si el dominio tiene un registro de DNS tipo MX, el sistema propone una serie de direcciones de correo electrónico estándar como webmaster@dominio o hostmaster@dominio para que el usuario elija una o solicita que el usuario escriba una con ese dominio |
| 4 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) elije una dirección propuesta o escribe su propia dirección de correo |
| 5 | El sistema envía un correo electrónico a la dirección propuesta por el usuario en el que se incluye un código de un solo uso para confirmar que el usuario está relacionado con ese dominio |
| 6 | El sistema se queda a la espera de que el usuario reciba el código de un solo uso |
| 7 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) confirma el código al sistema |
| 8 | El sistema solicita crear un registro TXT con un valor determinado en la zona DNS y se queda a la espera que el usuario confirme la creación |
| 9 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) confirma la creación del registro TXT en la zona DNS |
| 10 | El sistema confirma la existencia de un registro TXT en el dominio con el valor correcto y confirma la validación del dominio |
| **Postcondición** | El sistema asocia el nombre de dominio DNS a la cuenta del usuario | |
| **Excepciones** | **Paso** | **Acción** |
| 6 | Si el usuario no recibe el correo electrónico, el actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) solicita un nuevo código a una nueva dirección de correo electrónico, a continuación este caso de uso continúa |
| 10 | Si el sistema no puede confirmar la existencia de un registro TXT válido, el sistema solicita de nuevo al usuario la creación del registro TXT y vuelve a quedar a la espera, a continuación este caso de uso continúa |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0022** | **Validación de correo electrónico** | |
| **Versión** | 1.0 (30/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[CRQ-0005] Validación de identidad necesaria](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0005)   [[CRQ-0002] Correo electrónico autorizado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0002)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001)   [[IRQ-0008] Validación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0008)   [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario necesita confirmar que tiene acceso a una dirección de correo electrónico o durante la realización de los siguientes casos de uso: [[UC-0001] Registro de un usuario anónimo](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0001) | |
| **Precondición** | El usuario debe tener una dirección de correo válida | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) solicita la validación de una dirección de correo electrónico |
| 2 | El sistema solicita una dirección de correo al usuario |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) envía al sistema una dirección de correo electrónico |
| 4 | El sistema envía un correo electrónico a la dirección propuesta por el usuario en el que se incluye un código de un solo uso para confirmar que tiene acceso a esa dirección de correo electrónico |
| 5 | El sistema se queda a la espera de que el usuario reciba el código de un solo uso |
| 6 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) confirma el código al sistema |
| 7 | El sistema confirma la validez de la dirección de correo electrónico |
| **Postcondición** | El sistema asocia la dirección de correo electrónico a la cuenta del usuario | |
| **Excepciones** | **Paso** | **Acción** |
| 5 | Si el usuario no recibe el correo electrónico, el actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) solicita un nuevo código al sistema, a continuación este caso de uso continúa |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

##### Solicitud de certificados

Casos de uso relacionados con el proceso de solicitud y emisión de los certificados.

|  |  |  |
| --- | --- | --- |
| **UC-0005** | **Solicitud via web** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[CRQ-0004] Uso de certificados de usuario final](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0004)   [[CRQ-0001] Emisión solo a usuarios registrados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0001)   [[CRQ-0005] Validación de identidad necesaria](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0005)   [[CRQ-0006] Expiración antes que la AC Raíz](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0006)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001)   [[IRQ-0003] Solicitud de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0003)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004)   [[IRQ-0008] Validación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0008)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario solicita la emisión de un certificado mediante un formulario web. | |
| **Precondición** | El usuario debe estar registrado en el sistema, debe tener al menos una validación confirmada y debe haber generado una pareja de claves previamente | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) solicita al sistema emitir un nuevo certificado |
| 2 | El sistema muestra una lista de las posibles plantillas que el usuario puede solicitar |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) elige una de las plantillas |
| 4 | El sistema muestra al usuario los diferentes parámetros para el certificado solicitado que permite la plantilla |
| 5 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) rellena los parámetros de la plantilla |
| 6 | El sistema solicita la clave pública del nuevo certificado. Para ello solicita un CSR donde esté la clave pública. |
| 7 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) envía la clave pública mediante un CSR |
| 8 | El sistema comprueba que los datos recibidos son válidos respecto a la plantilla |
| 9 | El sistema recibe el CSR y comprueba que está bien formado |
| 10 | Si la plantilla permite la emisión automática del certificado, el sistema aprueba la solicitud y después emite el certificado |
| 11 | Si la plantilla no permite la emisión automática del certificado, se realiza el caso de uso [Emisión manual de un certificado (UC-0014)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0014) |
| **Postcondición** | El usuario recibe un certificado digital para la plantilla solicitada | |
| **Excepciones** | **Paso** | **Acción** |
| 8 | Si alguno de los datos recibidos no es correcto, el sistema notifica el error al usuario, a continuación este caso de uso queda sin efecto |
| 9 | Si el CSR recibido no está bien formado, el sistema comunica el error, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0023** | **Generar un CSR** | |
| **Versión** | 1.0 (01/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0003] Solicitud de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0003)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[CRQ-0004] Uso de certificados de usuario final](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0004) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario quiera generar un CSR y descargarlo a su PC para reutilizarlo en otro momento | |
| **Precondición** | El usuario debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) accede al sistema y solicita crear un CSR |
| 2 | El sistema solicita al usuario los detalles necesarios para generar un CSR, entre ellos, los detalles del nombre distinguido del certificado y el tamaño de la pareja de claves a generar |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) introduce los datos solicitados |
| 4 | El sistema el sistema valida que los datos son correctos y solicita al usuario cómo quiere obtener el CSR: generar el CSR remotamente y descargarlo; u obtener una sentencia de openssl para generarlo localmente |
| 5 | Si el usuario solicita generar el CSR remotamente, el sistema genera una nueva pareja de claves y un CSR y se lo da al usuario para descargar |
| 6 | Si el usuario solicita generar la sentencia de openssl, el sistema genera la sentencia openssl y se la muestra al usuario |
| **Postcondición** | El usuario recibe un archivo que contiene el CSR o bien el contenido del CSR para que lo pueda copiar | |
| **Excepciones** | **Paso** | **Acción** |
| 4 | Si alguno de los datos introducidos por el usuario no es correcto, el sistema comunica al usuario el error, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0007** | **Renovación via web** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[IRQ-0008] Validación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0008)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002)   [[CRQ-0006] Expiración antes que la AC Raíz](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0006)   [[IRQ-0003] Solicitud de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0003)   [[CRQ-0001] Emisión solo a usuarios registrados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0001)   [[CRQ-0005] Validación de identidad necesaria](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0005)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004)   [[CRQ-0003] Uso de certificados de operadores](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0003) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario solicita la renovación de un certificado que ya había solicitado cuando dicho certificado está cerca de la fecha de expiración. | |
| **Precondición** | El usuario debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) solicita al sistema la lista de certificados que ha solicitado y emitido |
| 2 | El sistema devuelve la lista de certificados que el usuario ha solicitado |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) elige uno de los certificados de la lista que ha expirado o que está próximo a que expire |
| 4 | El sistema busca la plantilla original y comprueba que es aún válida y que los datos del certificado concuerdan con los necesarios en la plantilla |
| 5 | El sistema comprueba si el certificado requiere alguna validación y que la validación aún está vigente |
| 6 | Si la plantilla permite la emisión automática del certificado, el sistema emite el certificado |
| 7 | Si la plantilla no permite la emisión automática del certificado, se realiza el caso de uso [Emisión manual de un certificado (UC-0014)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0014) |
| **Postcondición** | El usuario recibe un nuevo certificado digital que usa la plantilla del certificado original | |
| **Excepciones** | **Paso** | **Acción** |
| 4 | Si los datos del certificado no son adecuados para la plantilla original, el sistema comunica el error al usuario, a continuación este caso de uso queda sin efecto |
| 5 | Si el certificado requiere una validación y la validación ha expirado, el sistema comunica al usuario el error y le solicita que inicie de nuevo la validación requerida, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0017** | **Solicitud de un conjunto de certificados** | |
| **Versión** | 1.0 (27/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0011] Realizar validaciones previas a la emisión de un certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0011)   [[CRQ-0005] Validación de identidad necesaria](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0005)   [[CRQ-0001] Emisión solo a usuarios registrados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0001)   [[CRQ-0006] Expiración antes que la AC Raíz](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0006)   [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001)   [[CRQ-0003] Uso de certificados de operadores](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0003)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004)   [[CRQ-0004] Uso de certificados de usuario final](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0004)   [[IRQ-0003] Solicitud de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0003)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario solicita varios certificados de una sola vez, usando un formulario web para rellenar los detalles. | |
| **Precondición** | El usuario debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| - | - |
| **Postcondición** | El usuario recibe al menos uno de los certificados que ha solicitado | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

##### Emisión de certificados

Casos de uso relacionados con la emisión de los certificados.

|  |  |  |
| --- | --- | --- |
| **UC-0014** | **Emisión manual de un certificado** | |
| **Versión** | 1.0 (19/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0001] Emitir certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0001)   [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009)   [[OBJ-0010] Registro de validez de los certificados emitidos](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0010)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002)   [[CRQ-0006] Expiración antes que la AC Raíz](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0006)   [[IRQ-0003] Solicitud de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0003)   [[CRQ-0003] Uso de certificados de operadores](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#CRQ-0003) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador recibe una alerta sobre un certificado que se debe emitir manualmente. o durante la realización de los siguientes casos de uso: [[UC-0005] Solicitud via web](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0005), [[UC-0007] Renovación via web](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0007) | |
| **Precondición** | Existe una solicitud de emisión de certificado que necesita una emisión manual | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede al sistema y solicita al sistema la lista de certificados pendientes de emisión |
| 2 | El sistema devuelve la lista de los certificados que están pendientes de aprobación para su emisión |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige un certificado pendiente de emisión |
| 4 | El sistema devuelve los detalles del certificado y los detalles de la validación si los hubiera |
| 5 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) revisa todos los detalles del certificado y, si lo estima oportuno, autoriza la emisión del certificado |
| 6 | Si El operador aprueba la emisión del certificado, el sistema emite el certificado y notifica al solicitante |
| **Postcondición** | Se crea el certificado digital y se notifica al usuario que registró la solicitud | |
| **Excepciones** | **Paso** | **Acción** |
| 5 | Si el operador no autoriza la emisión del certificado, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) comunica al solicitante el rechazo de la emisión y marca la solicitud como rechazada, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

##### Revocación de certificados

Casos de uso relacionados con la revocación de los certificados emitidos por esta Autoridad de Certificación.

|  |  |  |
| --- | --- | --- |
| **UC-0008** | **Revocación por el usuario** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un usuario quiere que un certificado emitido sea revocado por esta autoridad de certificación | |
| **Precondición** | El usuario debe estar registrado en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) accede al sistema y solicita la lista de certificados que ha solicitado |
| 2 | El sistema devuelve la lista de certificados que el usuario ha solicitado y están emitidos |
| 3 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) elige uno de los certificados que están emitidos para solicitar su revocación |
| 4 | El sistema solicita al usuario un motivo para la revocación |
| 5 | El actor [Usuario registrado (ACT-0003)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0003) introduce un motivo y confirma la revocación del certificado |
| 6 | El sistema marca el certificado como revocado y le confirma la acción al usuario |
| **Postcondición** | El certificado queda revocado | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0009** | **Revocación por el operador** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002)   [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador inicia la revocación de un certificado | |
| **Precondición** | Debe existir un certificado emitido por la autoridad de certificación | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede al sistema y solicita al sistema realizar una búsqueda para revocar un certificado |
| 2 | El sistema devuelve los certificados que concuerdan con la búsqueda del operador |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona el certificado que quiere revocar de la lista de resultados |
| 4 | El sistema muestra los detalles del certificado y solicita al operador un motivo para la revocación |
| 5 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) introduce un motivo para la revocación y confirma la revocación del certificado |
| 6 | El sistema marca el certificado como revocado y notifica al solicitante de la revocación |
| **Postcondición** | El certificado queda revocado | |
| **Excepciones** | **Paso** | **Acción** |
| 2 | Si no existe ningún certificado que concuerde con la búsqueda, el sistema notifica que no hay coincidencias con la búsqueda, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0033** | **Republicar un certificado** | |
| **Versión** | 1.0 (15/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0002] Certificado emitido](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0002)   [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador inicia la republicación de un certificado, es decir, deshace la revocación de un certificado | |
| **Precondición** | Debe existir un certificado emitido y revocado por la autoridad de certificación | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede al sistema y solicita al sistema realizar una búsqueda para republicar un certificado |
| 2 | El sistema devuelve los certificados que concuerdan con la búsqueda del operador |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona el certificado que quiere republicar de la lista de resultados |
| 4 | El sistema muestra los detalles del certificado y solicita al operador confirmación para republicar el certificado |
| 5 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) confirma la republicación del certificado |
| 6 | El sistema quita la marca de revocación del certificado |
| **Postcondición** | El certificado deja de estar revocado | |
| **Excepciones** | **Paso** | **Acción** |
| 2 | Si no existe ningún certificado que concuerde con la búsqueda, el sistema notifica que no hay coincidencias con la búsqueda, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

##### Administración de plantillas

Casos de uso relacionados con la administración de plantillas de certificados.

|  |  |  |
| --- | --- | --- |
| **UC-0027** | **Buscar una plantilla** | |
| **Versión** | 1.0 (10/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004)   [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador necesita buscar una plantilla en la lista de plantillas disponibles o durante la realización de los siguientes casos de uso: [[UC-0012] Modificación de una plantilla](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0012), [[UC-0013] Eliminación de una plantilla](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0013), [[UC-0024] Restaurar una versión anterior de una plantilla](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0024), [[UC-0025] Duplicar una plantilla](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0025) | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede a la administración del sistema y accede al apartado de plantillas de certificados |
| 2 | El sistema muestra la lista de plantillas disponibles y opciones para crear una nueva o ver la lista de plantillas activas |
| 3 | Si el operador no encuentra la plantilla que busca, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) realiza un filtro sobre la lista de plantillas |
| **Postcondición** | El operador localiza una plantilla | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0011** | **Creación de una plantilla** | |
| **Versión** | 1.0 (19/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador quiere registrar una nueva plantilla de certificado digital | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede a la administración del sistema y accede al apartado de plantillas de certificados |
| 2 | El sistema muestra la lista de plantillas disponibles y opciones para crear una nueva o modificar una existente |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige crear una nueva plantilla |
| 4 | El sistema solicita un nombre para la nueva plantilla |
| 5 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) introduce el nombre para mostrar de la nueva plantilla |
| 6 | El sistema comprueba que no existe una plantilla con ese nombre y muestra al operador las opciones básicas de la plantilla como uso del certificado, tamaño mínimo de la clave y extensiones básicas |
| 7 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) introduce los campos solicitados y elige las opciones básicas para el certificado |
| 8 | El sistema el sistema solicita ahora otras opciones y extensiones adicionales |
| 9 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) introduce o selecciona las opciones o extensiones adicionales |
| 10 | El sistema solicita al operador que elija un método de validación de identidad |
| 11 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) el operador elige una validación si es necesario y finaliza el proceso |
| 12 | El sistema muesta todas las opciones seleccionadas al operador para que las revise y solicita confirmación para crear la plantilla |
| 13 | Si el operador confirma los detalles de la nueva plantilla, el sistema la almacena y establece el número de versión a 1 |
| **Postcondición** | Se crea una nueva plantilla en el sistema | |
| **Excepciones** | **Paso** | **Acción** |
| 13 | Si el operador no confirma los datos de la plantilla, el sistema omite la creación del certificado, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0012** | **Modificación de una plantilla** | |
| **Versión** | 1.0 (19/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador necesita modificar una plantilla de certificados | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas y debe existir al menos una plantilla en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | Se realiza el caso de uso [Buscar una plantilla (UC-0027)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0027) |
| 2 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la plantilla que quiere modificar |
| 3 | El sistema muestra los parámetros de la plantilla seleccionada para que el operador los pueda modificar |
| 4 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) modifica los parámetros de la plantilla que necesite y guarda los cambios |
| 5 | El sistema comprueba que los cambios son válidos y guarda los detalles de la plantilla, incrementando en uno la versión de la plantilla |
| **Postcondición** | La plantilla se actualiza en el sistema y su número de versión aumenta | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0013** | **Eliminación de una plantilla** | |
| **Versión** | 1.0 (19/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador necesita eliminar una plantilla de certificados | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas y debe existir al menos una plantilla en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | Se realiza el caso de uso [Buscar una plantilla (UC-0027)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0027) |
| 2 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la plantilla que quiere eliminar |
| 3 | El sistema muestra los parámetros de la plantilla seleccionada |
| 4 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la opción de eliminar la plantilla |
| 5 | El sistema solicita confirmación para eliminar la plantilla |
| 6 | Si el operador confirma la eliminación, el sistema marca la la plantilla seleccionada como eliminada |
| **Postcondición** | Se elimina la plantilla del sistema | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0018** | **Activar una plantilla** | |
| **Versión** | 1.0 (27/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004)   [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador quiere activar una plantilla de certificados digitales para que los usuarios finales puedan usarla para solicitar certificados | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas y debe existir al menos una plantilla en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede a la administración del sistema y accede al apartado de plantillas de certificados |
| 2 | El sistema muestra la lista de plantillas disponibles y opciones para crear una nueva o ver la lista de plantillas activas |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede a la lista de plantillas activas |
| 4 | El sistema muestra la lista de plantillas activas del sistema y opciones para activar una nueva plantilla |
| 5 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la opción de activar una plantilla existente |
| 6 | El sistema muestra la lista de las plantillas disponibles que aún no están activas |
| 7 | Si el operador no encuentra la plantilla que busca, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) realiza un filtro sobre la lista de plantillas |
| 8 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la plantilla que quiere activar |
| 9 | El sistema muestra algunos parámetros básicos de la plantilla seleccionada y solicita confirmación al operador |
| 10 | Si el operador confirma la activación de la plantilla, el sistema activa la plantilla |
| **Postcondición** | La plantilla se hace visible a los usuarios finales | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0026** | **Desactivar una plantilla** | |
| **Versión** | 1.0 (10/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador quiere desactivar una plantilla para que los usuarios finales no puedan solicitar certificados con dicha plantilla | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas y debe existir al menos una plantilla en el sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede a la administración del sistema y accede al apartado de plantillas de certificados |
| 2 | El sistema muestra la lista de plantillas disponibles y opciones para crear una nueva o ver la lista de plantillas activas |
| 3 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) accede a la lista de plantillas activas |
| 4 | El sistema muestra la lista de plantillas activas del sistema y opciones para activar una nueva plantilla |
| 5 | Si el operador no encuentra la plantilla que busca, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) realiza un filtro sobre la lista de plantillas activas |
| 6 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) elige la opción de desactivar una plantilla existente |
| 7 | El sistema solicita confirmación al operador para desactivar la plantilla elegida |
| 8 | Si el operador confirma la activación de la plantilla, el sistema desactiva la plantilla |
| **Postcondición** | La plantilla deja de ser visible para los usuarios | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0024** | **Restaurar una versión anterior de una plantilla** | |
| **Versión** | 1.0 (10/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004)   [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador quiere ver los parámetros de una versión anterior de una plantilla | |
| **Precondición** | El operador debe tener permisos para poder administrar plantillas | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | Se realiza el caso de uso [Buscar una plantilla (UC-0027)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0027) |
| 2 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona la plantilla de la que quiere ver su historial |
| 3 | El sistema muestra los parámetros de la plantilla |
| 4 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona la opción para ver el historial de la plantilla |
| 5 | El sistema muestra la lista de versiones de la plantilla |
| 6 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona una versión anterior |
| 7 | El sistema muestra los parámetros de la versión seleccionada para que el operador pueda comparar los cambios con la última versión |
| 8 | Si el operador quiere ver una versión diferente de la seleccionada, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona una versión diferente del historial y se vuelve al paso 7 |
| 9 | Si el operador decide restaurar la versión anterior que se está mostrando, el actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona la opción para restaurar la versión |
| 10 | El sistema solicita confirmación al operador para restaurar la versión elegida |
| 11 | Si el operador confirma la activación de la plantilla, el sistema realiza una copia de la versión de la plantilla a restaurar y establece su número de versión al número de versión más alto que haya de dicha plantilla más uno |
| **Postcondición** | La plantilla se actualiza en el sistema y su número de versión aumenta | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0025** | **Duplicar una plantilla** | |
| **Versión** | 1.0 (10/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0008] Administrar plantillas de certificados](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0008)   [[IRQ-0004] Plantilla de certificado](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0004) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un operador quiere duplicar una plantilla | |
| **Precondición** | El operador debe tener permisos para administrar plantillas y debe existir al menos una plantilla | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | Se realiza el caso de uso [Buscar una plantilla (UC-0027)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0027) |
| 2 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) selecciona la plantilla que quiere duplicar y elige la opción para duplicar dicha plantilla |
| 3 | El sistema crea una nueva plantilla copiando los parámetros de la plantilla seleccionada por el operador y le ofrece la oportunidad de modificarlos |
| 4 | El actor [Operador (ACT-0002)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0002) modifica los parámetros básicos, las extensiones y la validacion de la identidad de la nueva plantilla |
| 5 | El sistema muesta todas las opciones seleccionadas al operador para que las revise y solicita confirmación para crear la plantilla |
| 6 | Si el operador confirma los detalles de la nueva plantilla, el sistema la almacena y establece el número de versión a 1 |
| **Postcondición** | Se crea una nueva plantilla en el sistema | |
| **Excepciones** | **Paso** | **Acción** |
| 6 | Si el operador no confirma los datos de la plantilla, el sistema omite la creación del certificado, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

##### Configuración del servicio

Casos de uso relacionados con la instalación y configuración del servicio

|  |  |  |
| --- | --- | --- |
| **UC-0028** | **Configuración inicial de la autoridad de certificación** | |
| **Versión** | 1.0 (13/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0012] Administrar la autoridad de certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0012)   [[IRQ-0006] Autoridad de Certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0006) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando se quiere confirgurar la autoridad de certificación por primera vez | |
| **Precondición** | Se ha instalado el software y aún no se ha configurado la autoridad de certificación | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El sistema solicita los detalles del servidor de base de datos como nombre del servidor, nombre de la base de datos y la autenticación a usar |
| 2 | El actor [Instalador (ACT-0005)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0005) introduce los datos del servidor de base de datos |
| 3 | El sistema comprueba que los datos son correctos y que se puede conectar al servidor correctamente |
| 4 | El sistema solicita al usuario instalador si ya tiene un certificado de autoridad de certificación que quiera usar en esta CA o si quiere generar uno nuevo |
| 5 | Si el instalador indica tiene un certificado emitido, el sistema solicita la ruta donde puede encontrar el certificado |
| 6 | Si se debe generar un nuevo certificado, el sistema solicita los parámetros del certificado a generar |
| 7 | El sistema solicita algún detalle extra como el nombre de la autoridad de certificación |
| 8 | El actor [Instalador (ACT-0005)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0005) indica los detalles solicitados |
| 9 | El sistema indica que se va a generar un usuario administrador y se solicita una contraseña |
| 10 | El actor [Instalador (ACT-0005)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0005) proporciona la contraseña |
| 11 | El sistema muestra un resumen de todas las acciones que se van a llevar a cabo y los parámetros que se han proporcionado durante los pasos anteriores y solicita confirmación para continuar |
| 12 | El actor [Instalador (ACT-0005)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0005) confirma las acciones |
| 13 | El sistema realiza la configuración del sistema |
| **Postcondición** | La autoridad de certificación queda configurada para que se puedan empezar a emitir certificados | |
| **Excepciones** | **Paso** | **Acción** |
| 12 | Si el instalador no confirma las acciones a lleva a cabo, el sistema indica que no se va a llevar a cabo ninguna acción, a continuación este caso de uso queda sin efecto |
| 13 | Si la configuración inicial falla, el sistema notifica el error al instalador, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Este caso cubre los pasos de la configuración inicial del sistema:  - Configuración de la base de datos  - Configuración del certificado de la CA  - Creación del primer usuario administrador    TODO:  - Se podría crear una contraseña para poder añadir más servidores y podría ser la frase de paso del certificado de la CA | |

##### Configuración de la emisión

Casos de uso relacionados con la configuración de la emisión de certficados.

|  |  |  |
| --- | --- | --- |
| **UC-0032** | **Establecer las ubicaciones de los CPS** | |
| **Versión** | 1.0 (14/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | **?** | |
| **Dependencias** | Ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando **PD** | |
| **Precondición** | **PD** | |
| **Secuencia normal** | **Paso** | **Acción** |
| - | - |
| **Postcondición** | **PD** | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0031** | **Establecer la ubicación del servidor OCSP** | |
| **Versión** | 1.0 (14/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | **?** | |
| **Dependencias** | Ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el administrador quiere cambiar la ruta del servidor OCSP asociado al certificado de autoridad de certificación actual | |
| **Precondición** | Existe un servidor OCSP que da servicio al sistema | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) accede a la administración del sistema y accede a la sección de administración de la autoridad de certificación |
| 2 | El sistema muestra diferentes opciones para administrar la autoridad de certificación |
| 3 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) elige administrar los servidores OCSP |
| 4 | El sistema muestra los certificados de AC que hay en el sistema y muestra las URL de los servidores OCSP asociadas a cada uno |
| 5 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) elige añadir una nueva URL en el sistema |
| 6 | El sistema solicita la nueva URL |
| 7 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) introduce la nueva URL |
| 8 | El sistema comprueba que la URL es correcta y la asocia con el certificado actual de la autoridad de certificación |
| **Postcondición** | Se asocia una nueva URL para comprobación OCSP con el certificado actual | |
| **Excepciones** | **Paso** | **Acción** |
| 8 | Si la URL introducida no es correcta, el sistema muestra el error al administrador, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Un administrador puede elegir cambiar la URL del servidor OCSP de los certificados que se van a emitir desde el momento del cambio. Aun así, hay que mantener un historial de todas las URLs que se han usado ya que si hay algún certificado emitido con una URL anterior, hasta que el certificado expire la URL debe seguir siendo válida. | |

|  |  |  |
| --- | --- | --- |
| **UC-0030** | **Establecer la ubicación de las CRL** | |
| **Versión** | 1.0 (14/04/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** | Ninguno | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el administrador quiera cambiar la ubicación de las CRL asociadas al certificado de AC actual | |
| **Precondición** | La nueva ubicación debe ser válida | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) accede a la administración del sistema y accede a la sección de administración de la autoridad de certificación |
| 2 | El sistema muestra diferentes opciones para administrar la autoridad de certificación |
| 3 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) elige administrar las ubicaciones de las CRL |
| 4 | El sistema muestra los certificados de AC que hay en el sistema y muestra las ubicaciones de las CRL asociadas a cada uno |
| 5 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) modifica las ubicaciones de las CRL del certificado actual |
| 6 | El sistema comprueba que las ubicaciones son válidas y asocia las nuevas ubicaciones con el certificado de AC actual |
| 7 | Si alguna ubicación anterior se eliminara y hubiera algún certificado que tenga esa ubicación en su extensión CRL, el sistema mantiene la ubicación eliminada en el historial de ubicaciones |
| **Postcondición** | El sistema asocia la nueva ubicación al certificado actual | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Un administrador puede elegir cambiar la ubicación de las CRL de los certificados que se van a emitir desde el momento del cambio. Aun así, hay que mantener un historial de todas las ubicaciones que se han usado ya que si hay algún certificado emitido con una ubicación anterior, hasta que el certificado expire la ubicación debe seguir siendo válida. | |

|  |  |  |
| --- | --- | --- |
| **UC-0016** | **Cambio del certificado de la AC** | |
| **Versión** | 1.0 (27/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[IRQ-0006] Autoridad de Certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0006)   [[OBJ-0012] Administrar la autoridad de certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0012) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un administrador quiere cambiar el certificado de la autoridad de certificación o durante la realización de los siguientes casos de uso: [[UC-0010] Revocación de la autoridad de certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0010) | |
| **Precondición** | El administrador debe tener un nuevo certificado digital válido que se pueda usar para firmar nuevos digitales | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) accede a la administración del sistema y accede a la sección de administración de la autoridad de certificación |
| 2 | El sistema muestra diferentes opciones para administrar la autoridad de certificación |
| 3 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) solicita cambiar el certificado de la autoridad de certificación |
| 4 | El sistema muestra información sobre lo que implica este cambio y solicita continuar con el cambio |
| 5 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) confirma que quiere seguir adelante con el cambio |
| 6 | El sistema solicita al administrador que proporcione el nuevo certificado de la autoridad de certificación y su pareja de claves asociada |
| 7 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) proporciona el nuevo certificado y la pareja de claves asociada |
| 8 | El sistema confirma que el certificado es válido para el propósito que se necesita y comprueba que es consistente con las plantillas que están definidas en el sistema |
| 9 | El sistema indica que el nuevo certificado es válido y vuelve a solicitar confirmación al administrador para hacer el cambio. Además, puede dar la opción al administrador opciones para: - volver a reemitir los certificados aún válidos emitidos por el certificado anterior - revocar los certificados anteriores - dejar de generar CRLs para el certificado anterior |
| 10 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) confirma que quiere realizar el cambio y, si hiciera falta, reemitir o revocar los certificados ya emitidos. |
| 11 | El sistema aplica los cambios necesarios para cambiar el certificado y la pareja de claves de la autoridad de certificación de acuerdo con el procedimiento acordado |
| 12 | Si el administrador eligió reemitir los certificados previos, el sistema vuelve a emitir los certificados asociados a la pareja de claves anterior |
| 13 | Si el administrador eligió revocar los certificados previos, el sistema revoca los certificados emitidos por el certificado anterior |
| 14 | Si el administrador eligió dejar de generar CRLs para el certificado anterior, el sistema dejará de generar CRLs firmadas con el certificado anterior |
| **Postcondición** | El certificado de la autoridad de certificación cambia y desde ese momento los nuevos certificados emitidos por la AC estarán firmados por el nuevo certificado | |
| **Excepciones** | **Paso** | **Acción** |
| 8 | Si si el nuevo certificado es incompatible con alguna plantilla existente, el sistema notifica al administrador que el certificado no es válido ya que hay plantillas que funcionarán con él, a continuación este caso de uso queda sin efecto |
| 10 | Si el administrador no confirma los cambios, el sistema no realiza ningún cambio en la autoridad de certificación, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **UC-0010** | **Revocación de la autoridad de certificación** | |
| **Versión** | 1.0 (16/02/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0002] Revocar certificados digitales](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0002)   [[OBJ-0012] Administrar la autoridad de certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0012)   [[IRQ-0006] Autoridad de Certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0006) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un administrador de la autoridad de certificación inicia la revocación de la autoridad de certificación | |
| **Precondición** | Se decide revocar el certificado de la autoridad de certificación | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) accede a la administración del sistema y accede a la sección de administración de la autoridad de certificación |
| 2 | El sistema muestra diferentes opciones para administrar la autoridad de certificación |
| 3 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) elige la opción para revocar la autoridad de certificación |
| 4 | El sistema muestra una descripción de las acciones que se van a llevar a cabo, como revocar todos los certificados emitidos y las consecuencias de hacerlo y solicita confirmación al usuario dos veces |
| 5 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) confirma las dos veces la revocación de la autoridad de certificación |
| 6 | El sistema revoca todos los certificados emitidos por esta autoridad de certificación |
| 7 | El sistema genera una última lista de revocación de certificados |
| 8 | El sistema confirma los cambios hechos al administrador y solicita al administrador si quiere cambiar el certificado de la autoridad de certificación |
| 9 | Si el administrador confirma que quiere cambiar el certificado de la autoridad de certificación, se realiza el caso de uso [Cambio del certificado de la AC (UC-0016)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20#UC-0016) |
| **Postcondición** | El certificado de la autoridad de certificación queda revocado | |
| **Excepciones** | **Paso** | **Acción** |
| - | - |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | La revocación de un certificado de CA es un caso raro y debería ser una excepción. Probablemente el mejor plan de acción es revocar todos los certificados emitidos por el certificado de la CA, dejar de usarlo y así dejar que el certificado de la CA expire. | |

|  |  |  |
| --- | --- | --- |
| **UC-0020** | **Cambiar el rol de un operador** | |
| **Versión** | 1.0 (27/03/2018) | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Fuentes** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#STK-0001) | |
| **Dependencias** |  [[OBJ-0012] Administrar la autoridad de certificación](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0012)   [[IRQ-0001] Usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0001)   [[IRQ-0007] Rol de usuario](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#IRQ-0007)   [[OBJ-0009] Llevar un registro de los usuarios del sistema](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#OBJ-0009) | |
| **Descripción** | El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando un administrador quiere cambiar el rol de un operador | |
| **Precondición** | Debe existir al menos un operador en la autoridad de certificación | |
| **Secuencia normal** | **Paso** | **Acción** |
| 1 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) accede a la administración del sistema y accede a la sección de permisos de los usuarios |
| 2 | El sistema solicita al administrador un detalle del usuario para realizar una búsqueda |
| 3 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) introduce una cadena de texto que pueda servir para identificar al usuario, como el nombre, apellido o nombre de usuario |
| 4 | El sistema realiza una búsqueda entre los operadores de la autoridad de certificación y devuelve una lista de aquellos que coincidan con los criterios de búsqueda |
| 5 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) selecciona el usuario del operador que quiere modificar |
| 6 | El sistema muestra los detalles del operador y opciones para administrar esta cuenta |
| 7 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) elige la opción de modificar los permisos del usuario |
| 8 | El sistema muestra los diferentes permisos que hay disponibles y aquellos que ya están asignados al usuario |
| 9 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) realiza los cambios que necesite en los permiosos del usuario, añadiendo o quitando según estime oportuno y guarda los cambios |
| 10 | El sistema comprueba que los permisos nuevos tienen sentido y pide confirmación al administrador para hacer el cambio |
| 11 | El actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) confirma los cambios |
| 12 | El sistema aplica los cambios en los permisos del usuario |
| **Postcondición** | Los permisos del operador cambian | |
| **Excepciones** | **Paso** | **Acción** |
| 4 | Si no se devuelve ningún resultado en la búsqueda, el actor [Administrador (ACT-0001)](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_CRS.html#ACT-0001) debe realizar una nueva búsqueda con unos términos diferentes, a continuación este caso de uso continúa |
| 11 | Si el administrador no confirma los cambios, el sistema no guarda los cambios en los permisos del usuario, a continuación este caso de uso queda sin efecto |
| **Rendimiento** | **Paso** | **Tiempo máximo** |
| - | - |
| **Frecuencia esperada** | **PD** | |
| **Importancia** | **PD** | |
| **Urgencia** | **PD** | |
| **Estado** | **PD** | |
| **Estabilidad** | **PD** | |
| **Comentarios** | Ninguno | |

## Matrices de rastreabilidad

**Matriz de rastreabilidad**: Objetivo - Requisito de información

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| TRM-0003 | [OBJ-0001](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0001) | [OBJ-0002](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0002) | [OBJ-0008](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0008) | [OBJ-0009](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0009) | [OBJ-0010](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0010) | [OBJ-0011](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0011) | [OBJ-0012](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#OBJ-0012) |
| [IRQ-0001](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0001) | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - |
| [IRQ-0002](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0002) | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| [IRQ-0003](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0003) | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |
| [IRQ-0004](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0004) | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |
| [IRQ-0006](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0006) | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - |
| [IRQ-0007](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0007) | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - |
| [IRQ-0008](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#IRQ-0008) | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |

**Matriz de rastreabilidad**: Objetivo - Caso de uso

| TRM-0002 | OBJ-0001 | OBJ-0002 | OBJ-0008 | OBJ-0009 | OBJ-0010 | OBJ-0011 | OBJ-0012 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| UC-0001 | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| UC-0002 | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| UC-0003 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - |
| [UC-0004](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20#UC-0004) | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - |
| UC-0005 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| UC-0007 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| UC-0008 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - |
| UC-0009 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - |
| UC-0010 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif |
| UC-0011 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0012 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0013 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0014 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| UC-0016 | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif |
| UC-0017 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |
| UC-0018 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0020 | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif |
| UC-0021 | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |
| UC-0022 | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |
| UC-0023 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - |
| UC-0024 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0025 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0026 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0027 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0028 | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif |
| UC-0030 | - | - | - | - | - | - | - |
| UC-0031 | - | - | - | - | - | - | - |
| UC-0032 | - | - | - | - | - | - | - |
| UC-0033 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - |

**Matriz de rastreabilidad**: Objetivo – Restricción

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| TRM-0001 | OBJ-0001 | OBJ-0002 | OBJ-0008 | OBJ-0009 | OBJ-0010 | OBJ-0011 | OBJ-0012 |
| CRQ-0001 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - |
| CRQ-0002 | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - |
| CRQ-0003 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif |
| CRQ-0004 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - |
| CRQ-0005 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - |
| CRQ-0006 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| CRQ-0007 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - |

**Matriz de rastreabilidad**: Operación - Caso de uso

| TRM-0004 | SOP-0001 | SOP-0002 | SOP-0003 | SOP-0004 | SOP-0005 | SOP-0006 | SOP-0007 | SOP-0008 | SOP-0009 | SOP-0010 | SOP-0011 | SOP-0012 | SOP-0013 | SOP-0014 | SOP-0015 | SOP-0016 | SOP-0017 | SOP-0018 | SOP-0019 | SOP-0020 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| UC-0001 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0002 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0003 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0004 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0005 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0007 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0008 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0009 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0010 | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0011 | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0012 | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0013 | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - |
| UC-0014 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0016 | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - |
| UC-0017 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0018 | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0020 | - | - | - | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - |
| UC-0021 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif |
| UC-0022 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - |
| UC-0023 | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0024 | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0025 | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0026 | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - |
| UC-0027 | - | - | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - |
| UC-0028 | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - |
| UC-0030 | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - |
| UC-0031 | - | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - |
| UC-0032 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - |
| UC-0033 | - | - | C:\Tools\REM 1.2.2\xml\default\trace.gif | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |

## Análisis del sistema

### Tipos

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0004** | **Key** | | |
| **Versión** | 1.0 (13/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa una clave en una pareja de claves | | |
| **Supertipo** | Ninguno | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| - | - | - |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **Key:: Contents** |
| **Descripción** | Este atributo representa contenido de la clave codificado en base64 |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **Key:: Type** |
| **Descripción** | Este atributo representa el tipo de la clave, es decir, el algoritmo usado para generar la clave |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0002** | **CertificateRequest** | | |
| **Versión** | 1.0 (13/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa una solicitud para obtener un certificado digital | | |
| **Supertipo** | Ninguno | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| User | User | 1 |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateRequest:: DistinguishedName** |
| **Descripción** | Este atributo representa el nombre distinguido para el que se solicita un certificado |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateRequest:: Contents** |
| **Descripción** | Este atributo representa la solicitud CSR en formato PKCS#10 codificada en base64 |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0005** | **CertificateTemplate** | | |
| **Versión** | 1.0 (14/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa una plantilla para crear certificados digitales | | |
| **Supertipo** | Ninguno | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| CertificatePolicies | Sequence(CertificatePolicyInformation) | 1.. MAX |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: Name** |
| **Descripción** | Este atributo representa el nombre de esta plantilla en el sistema |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: Days** |
| **Descripción** | Este atributo representa el número de días que el certificado será válido |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: Enabled** |
| **Descripción** | Este atributo representa la plantilla puede ser usada por los usuarios finales |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: Version** |
| **Descripción** | Este atributo representa número de versión |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: MinBits** |
| **Descripción** | Este atributo representa el número mínimo de bits para el tamaño de la pareja de claves |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: BasicConstraints** |
| **Descripción** | Este atributo representa indica si el certificado es de una CA o entidad final y la longitud máxima de la cadena de certificados bajo este certificado |
| **Tipo** | BasicConstraints |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: KeyUsage** |
| **Descripción** | Este atributo representa para qué se puede usar el certificado |
| **Tipo** | Sequence(String) |
| **Comentarios** | Valores posibles: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly and decipherOnly |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: ExtendedKeyUsage** |
| **Descripción** | Este atributo representa lista de OID que indica el propósito del certificado |
| **Tipo** | Sequence(OID) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: CRLDistributionPoint** |
| **Descripción** | Este atributo representa la lista de URLs para obtener la CRL |
| **Tipo** | Sequence(String) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: AIA** |
| **Descripción** | Este atributo representa la lista de URLs del Authority Information Access (OCSP) |
| **Tipo** | Sequence(String) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: SigningAlgorithm** |
| **Descripción** | Este atributo representa el algoritmo usado para firmar |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificateTemplate:: AutoSign** |
| **Descripción** | Este atributo representa si los certificados que usan esta plantilla se emiten automáticamente |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0001** | **Certificate** | | |
| **Versión** | 1.0 (13/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa un certificado digital emitido por la autoridad de certificación | | |
| **Supertipo** | Ninguno | | |
| **Subtipos (disjuntos)** |  [[TYP-0006] RevokedCertificate](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%09%09%09%09%09%09%09%09%09%09#TYP-0006) | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| User | User | 1 |
| Template | CertificateTemplate | 1 |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **Certificate:: Subject** |
| **Descripción** | Este atributo representa el sujeto del certificado |
| **Tipo** | String |
| **Valor inicial** | Sujeto del certificado |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **Certificate:: X509** |
| **Descripción** | Este atributo representa el certificado emitido codificado en formato base64 |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **Certificate:: StartDate** |
| **Descripción** | Este atributo representa la fecha de inicio de validez |
| **Tipo** | Date |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **Certificate:: EndDate** |
| **Descripción** | Este atributo representa la fecha de fin de validez |
| **Tipo** | Date |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **Certificate:: SerialNumber** |
| **Descripción** | Este atributo representa número de serie único para este certificado |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0006** | **RevokedCertificate** | | |
| **Versión** | 1.0 (14/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa un certificado que está revocado | | |
| **Supertipo** | [[TYP-0001] Certificate](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\%0a%09%09%09%09%09%09%09%09#TYP-0001) | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| - | - | - |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **RevokedCertificate:: RevokedDate** |
| **Descripción** | Este atributo representa la fecha de la revocación de este certificado |
| **Tipo** | Date |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **RevokedCertificate:: RevocationReason** |
| **Descripción** | Este atributo representa la razón por la que el certificado está revocado |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0007** | **CertificatePolicyInformation** | | |
| **Versión** | 1.0 (14/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa una estructura para registrar normas de emisión de certificados | | |
| **Supertipo** | Ninguno | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| - | - | - |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificatePolicyInformation:: PolicyId** |
| **Descripción** | Este atributo representa el OID de esta norma |
| **Tipo** | OID |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **CertificatePolicyInformation:: Qualifiers** |
| **Descripción** | Este atributo representa la lista de normas que incluye la extensión |
| **Tipo** | Sequence(PolicyQualifier) |
| **Comentarios** | Ninguno |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0008** | **User** | | |
| **Versión** | 1.0 (14/04/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa un usuario del sistema | | |
| **Supertipo** | Ninguno | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| - | - | - |
| **Comentarios** | Ninguno | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **TYP-0009** | **Group** | | |
| **Versión** | 1.0 (18/05/2018) | | |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) | | |
| **Dependencias** | Ninguno | | |
| **Descripción** | Este tipo de objetos representa un grupo de usuarios | | |
| **Supertipo** | Ninguno | | |
| **Subtipos** | Ninguno | | |
| **Componentes** | **Nombre** | **Tipo** | **Multiplicidad** |
| Members | Set(User) | 0.. MAX |
| **Comentarios** | Ninguno | | |

|  |  |
| --- | --- |
| **Atributo variable** | **Group:: Name** |
| **Descripción** | Este atributo representa el nombre del grupo |
| **Tipo** | String |
| **Comentarios** | Ninguno |

### Tipos valor

|  |  |
| --- | --- |
| **VAL-0002** | **OID** |
| **Versión** | 1.0 (14/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa un Object Identifier de ASN.1 |
| **Definición** | PD |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **VAL-0001** | **X509Extension** |
| **Versión** | 1.0 (14/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa una extensión para un certificado, CRL o CSR |
| **Definición** | PD |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **X509Extension:: OID** |
| **Descripción** | Este atributo representa el identificador de la extensión |
| **Tipo** | OID |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **X509Extension:: Value** |
| **Descripción** | Este atributo representa Valor de la extensión |
| **Tipo** | String |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **X509Extension:: Critical** |
| **Descripción** | Este atributo representa la criticidad de la extensión |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **VAL-0003** | **PolicyQualifier** |
| **Versión** | 1.0 (15/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa una norma que sigue la AC para emitir certificados |
| **Definición** | PD |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **PolicyQualifier:: Identifier** |
| **Descripción** | Este atributo representa el OID que identifica esta norma |
| **Tipo** | OID |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **PolicyQualifier:: Value** |
| **Descripción** | Este atributo representa la lista de políticas de este cualificador (CPS o UserNotice) |
| **Tipo** | Sequence(String) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **VAL-0004** | **BasicConstraints** |
| **Versión** | 1.0 (15/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa un valor que identifica si el certificado es un certificado de AC |
| **Definición** | PD |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **BasicConstraints:: CA** |
| **Descripción** | Este atributo representa un booleano que indica si el certificado es de una AC o no |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **BasicConstraints:: PathLength** |
| **Descripción** | Este atributo representa el número máximo de certificados auto-firmados que puede haber entre este certificado y uno de entidad final |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **VAL-0005** | **KeyUsage** |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa el valor de la extensión KeyUsage de X509 |
| **Definición** |  |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **KeyUsage:: Value** |
| **Descripción** | Este atributo representa los valores posibles de la extensión |
| **Tipo** | Sequence(String) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **KeyUsage:: Critical** |
| **Descripción** | Este atributo representa si esta extensión es crítica o no |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **VAL-0006** | **ExtendedKeyUsage** |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa el valor de la extensión ExtendedKeyUsage de X509 |
| **Definición** | PD |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **ExtendedKeyUsage:: Value** |
| **Descripción** | Este atributo representa los valores posibles de la extensión |
| **Tipo** | Sequence(String) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **ExtendedKeyUsage:: Critical** |
| **Descripción** | Este atributo representa si esta extensión es crítica o no |
| **Tipo** | Integer |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **VAL-0007** | **Permission** |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo valor representa un permiso que se puede asignar a un usuario |
| **Definición** |  |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **Permission:: Name** |
| **Descripción** | Este atributo representa el nombre del permiso |
| **Tipo** | String |
| **Comentarios** | Ninguno |

### Asociaciones

Las asociaciones representan una relación entre dos tipos.

|  |  |
| --- | --- |
| **ASO-0001** | **RevocationList(Certificate, RevokedCertificate)** |
| **Versión** | 1.0 (14/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Este tipo de asociación representa el hecho de que una lista de revocación de certificados |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Rol variable** | **RevocationList(Certificate, RevokedCertificate):: SingingCertificate** |
| **Descripción** | Este rol representa el certificado que firma la CRL |
| **Tipo** | Certificate |
| **Multiplicidad** | 1 |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Rol variable** | **RevocationList(Certificate, RevokedCertificate):: Certificates** |
| **Descripción** | Este rol representa la lista de los certificados revocados |
| **Tipo** | Sequence(RevokedCertificate) |
| **Multiplicidad** | 0.. MAX |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **RevocationList(Certificate, RevokedCertificate):: CreateDate** |
| **Descripción** | Este atributo representa la fecha de la emisión |
| **Tipo** | Date |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **RevocationList(Certificate, RevokedCertificate):: NextUpdate** |
| **Descripción** | Este atributo representa la fecha de la siguiente emisión |
| **Tipo** | Date |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **RevocationList(Certificate, RevokedCertificate):: ExtensionList** |
| **Descripción** | Este atributo representa la lista de extensiones de esta CRL |
| **Tipo** | Set(X509Extension) |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Atributo variable** | **RevocationList(Certificate, RevokedCertificate):: SigningAlgorithm** |
| **Descripción** | Este atributo representa el algoritmo usado para firmar |
| **Tipo** | String |
| **Comentarios** | Ninguno |

## Operaciones del sistema

### Criptografía

|  |  |
| --- | --- |
| **SOP-0004** | **CreateCSR** |
| **Tipo del resultado** | CertificateRequest |
| **Versión** | 1.0 (13/04/2018) |
| **Autores** | [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Genera un nuevo CSR a partir de una clave pública y un nombre distinguido |
| **Parámetros** | distinguishedName : String -- el nombre distinguido para el que se solicita un certificado publicKey : Key -- la clave pública para la que se crea el certificado |
| **Expresiones de precondición** | **Formato del DN**: distinguishedName debe ser un nombre distinguido en el formato correcto |
| **Expresiones de precondición (OCL)** | **Formato del DN**: true |
| **Expresiones de postcondición** | Ninguno |
| **Expresiones de postcondición (OCL)** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0001** | **CreateCertificate** |
| **Tipo del resultado** | Certificate |
| **Versión** | 1.0 (13/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Genera un certificado digital desde un CSR |
| **Parámetros** | csr : CertificateRequest -- una solicitud de certificado template : CertificateTemplate -- la plantilla que define las características del certificado a emitir |
| **Expresiones de precondición** | **csr**: csr debe ser un CSR codificado en base 64 válido **plantilla**: La plantilla debe ser una plantilla activa en el sistema |
| **Expresiones de precondición (OCL)** | **csr**: true **plantilla**: true |
| **Expresiones de postcondición** | **certificado**: El certificado emitido se añade a la lista de certificados emitidos de la AC y se asocia con el usuario que lo ha solicitado |
| **Expresiones de postcondición (OCL)** | **certificado**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0002** | **RevokeCertificate** |
| **Tipo del resultado** | Booleano |
| **Versión** | 1.0 (13/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Revoca un certificado |
| **Parámetros** | certificate : Certificate -- el certificado que se quiere revocar reason : String -- la razón por la que se revoca el certificado |
| **Expresiones de precondición** | **certificado**: El certificado que se quiere revocar no debe haber expirado |
| **Expresiones de precondición (OCL)** | **certificado**: true |
| **Expresiones de postcondición** | **certificado**: El certificado se añade a a lista de revocación de certificados de la AC |
| **Expresiones de postcondición (OCL)** | **certificado**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0003** | **RefreshCRL** |
| **Tipo del resultado** | RevocationList |
| **Versión** | 1.0 (13/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Crea una CRL nueva para un certificado de AC |
| **Parámetros** | forCertificate : Certificate -- la CRL incluye los certificados revocados firmados por este certificado nextUpdate : Date -- la fecha de la siguiente emisión |
| **Expresiones de precondición** | **forCertificate**: El certificado usado para firmar la CRL debe ser aún válido **nextUpdate**: La fecha de la siguiente actualización no puede haber pasado ya |
| **Expresiones de precondición (OCL)** | **forCertificate**: true **nextUpdate**: true |
| **Expresiones de postcondición** | Ninguno |
| **Expresiones de postcondición (OCL)** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0005** | **UnrevokeCertificate** |
| **Tipo del resultado** | Certificate |
| **Versión** | 1.0 (15/04/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Quita la marca de revocación de un certificado revocado |
| **Parámetros** | certificate : RevokedCertificate -- certificado revocado que se quiere publicar |
| **Expresiones de precondición** | **certificate**: 'certificate' debe ser un certificado revocado cuya fecha de fin de validez no haya pasado aún y cuyo motivo de revocación sea certificateHold |
| **Expresiones de precondición (OCL)** | **certificate**: true |
| **Expresiones de postcondición** | **certificado**: El certificado se quita de la lista de certificados revocados |
| **Expresiones de postcondición (OCL)** | **certificado**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **UnrevokeCertificate::CertificateExpired** |
| **Condición** | La fecha de fin de validez ha pasado ya |
| **Condición (OCL)** | false |
| **Expresión** | No tiene sentido revocar un certificado que ha expirado |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

### Plantillas

|  |  |
| --- | --- |
| **SOP-0006** | **SaveTemplate** |
| **Tipo del resultado** | Template |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | **PD** |
| **Parámetros** | days : Integer -- el número de días que un certificado es válido basicConstraints : BasicConstraints -- el valor de la extensión BasicConstraints keyUsage : KeyUsage -- el valor de la extensión KeyUsage extendedKeyUsage : ExtendedKeyUsage -- el valor de la extensión ExtendedKeyUsage enabled : Integer -- si la extensión debe ser visible para los usuarios groups : Set(Group) -- el conjunto de grupos de usuarios que tienen acceso a esta plantilla policies : Set(CertificatePolicyInformation) -- la lista de detales de normas que se incluirá en la extensión CertificatePolicies |
| **Expresiones de precondición** | Ninguno |
| **Expresiones de precondición (OCL)** | true |
| **Expresiones de postcondición** | **template**: Se crea una nueva plantilla en el sistema |
| **Expresiones de postcondición (OCL)** | **template**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **SaveTemplate::ValueError** |
| **Condición** | Si el valor de basicConstraints y keyUsage no es consistente |
| **Condición (OCL)** | false |
| **Expresión** | **PD** |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0007** | **EnableTemplate** |
| **Tipo del resultado** | Template |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Activa una plantilla |
| **Parámetros** | template : CertificateTemplate -- la plantilla que se desea activar |
| **Expresiones de precondición** | **template**: La plantilla debe existir en el sistema |
| **Expresiones de precondición (OCL)** | **template**: true |
| **Expresiones de postcondición** | **template**: La plantilla queda activada y los usuarios con permiso pueden usarla |
| **Expresiones de postcondición (OCL)** | **template**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **EnableTemplate::TemplateError** |
| **Condición** | La plantilla no existe en el sistema |
| **Condición (OCL)** | false |
| **Expresión** | **PD** |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0008** | **DisableTemplate** |
| **Tipo del resultado** | Template |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Desactiva una plantilla |
| **Parámetros** | template : CertificateTemplate -- la plantilla que se desea desactivar |
| **Expresiones de precondición** | **template**: La plantilla debe existir en el sistema |
| **Expresiones de precondición (OCL)** | **template**: true |
| **Expresiones de postcondición** | **template**: La plantilla queda desactivada y los usuarios dejan de poder usarla |
| **Expresiones de postcondición (OCL)** | **template**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **DisableTemplate::TemplateError** |
| **Condición** | La plantilla no existe en el sistema |
| **Condición (OCL)** | false |
| **Expresión** | **PD** |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0009** | **RemoveTemplate** |
| **Tipo del resultado** | void |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Elimina una plantilla del sistema |
| **Parámetros** | template : CertificateTemplate -- la plantilla que se desea eliminar |
| **Expresiones de precondición** | **template**: La plantilla debe existir en el sistema |
| **Expresiones de precondición (OCL)** | **template**: true |
| **Expresiones de postcondición** | **template**: La plantilla queda eliminada, así como todas las versiones anteriores que pudiera haber |
| **Expresiones de postcondición (OCL)** | **template**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **RemoveTemplate::TemplateError** |
| **Condición** | La plantilla no existe en el sistema |
| **Condición (OCL)** | false |
| **Expresión** | **PD** |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0013** | **FindTemplate** |
| **Tipo del resultado** | Set(CertificateTemplate) |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Filtra la lista de plantillas del sistema |
| **Parámetros** | query : String -- una cadena de texto que se usa para filtrar la lista de plantillas |
| **Expresiones de precondición** | **templates**: Debe existir al menos una plantilla en el sistema |
| **Expresiones de precondición (OCL)** | **templates**: true |
| **Expresiones de postcondición** | **results**: se devuelve una lista de plantillas cuyos nombres coinciden con la consulta de búsqueda |
| **Expresiones de postcondición (OCL)** | **results**: true |
| **Comentarios** | Ninguno |

### Configuración CA

|  |  |
| --- | --- |
| **SOP-0010** | **SetupCertificate** |
| **Tipo del resultado** | Certificate |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Establece el certificado de la CA, el que se usará para firmar los certificados generados por esta CA |
| **Parámetros** | certificate : Certificate -- el nuevo certificado de la CA key : Key -- la clave privada del nuevo certificado de la CA |
| **Expresiones de precondición** | **key-certificate**: La clave privada key y la clave pública del certificado deben corresponderse |
| **Expresiones de precondición (OCL)** | **key-certificate**: true |
| **Expresiones de postcondición** | **certificate**: Se configura la CA para que use la nueva pareja clave/certificado para firmar las solicitudes de los usuarios |
| **Expresiones de postcondición (OCL)** | **certificate**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **SetupCertificate::key-certificate** |
| **Condición** | La pareja clave privada/certificado no se corresponden |
| **Condición (OCL)** | false |
| **Expresión** | La clave pública del certificado 'certificate' no se corresponde con la clave privada de 'key' |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0011** | **SetupCRL** |
| **Tipo del resultado** | void |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Configura la generación de CRL |
| **Parámetros** | days : Integer -- la frecuencia de actualización de las CRLs en días uRLs : Set(String) -- la lista de URLs donde se pueden descargar las CRLs y que se añadirán en los certificados emitidos por la CA path : String -- la ruta en el sistema donde se guardará el archivo .crl con la lista de revocación de certificados |
| **Expresiones de precondición** | **days**: days debe ser mayor estricto de 0 |
| **Expresiones de precondición (OCL)** | **days**: true |
| **Expresiones de postcondición** | **crl**: el sistema generará una nueva CRL cada 'days' días y añadirá en la extensión CDP las URLs que haya en uRLs |
| **Expresiones de postcondición (OCL)** | **crl**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **SetupCRL::PathNotFoundError** |
| **Condición** | la ruta de exportación no es accesible por el sistema |
| **Condición (OCL)** | false |
| **Expresión** | **PD** |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0012** | **SetupOCSP** |
| **Tipo del resultado** | void |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Configura las rutas OCSP |
| **Parámetros** | uRL : Date -- la URL que se añadirá en la extensión AIA de los certificados emitidos por la CA certURL : String -- La URL donde se puede descargar el certificado que firma las respuestas OCSP |
| **Expresiones de precondición** | Ninguno |
| **Expresiones de precondición (OCL)** | true |
| **Expresiones de postcondición** | **aia**: La extensión AIA de los certificados emitidos incluirá la URL del servidor OCSP 'uRL' y la URL 'certURL' del certificado que firma las respuestas OCSP |
| **Expresiones de postcondición (OCL)** | **aia**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0015** | **AddCertificatePolicy** |
| **Tipo del resultado** | CertificatePolicyInformation |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Añade una descripción de norma de emisión de certificados |
| **Parámetros** | policyInformation : RevocationList -- los detalles de la norma a almacenar |
| **Expresiones de precondición** | Ninguno |
| **Expresiones de precondición (OCL)** | true |
| **Expresiones de postcondición** | **policy**: La información de la norma queda registrada en el sistema |
| **Expresiones de postcondición (OCL)** | **policy**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0016** | **RemoveCertificatePolicy** |
| **Tipo del resultado** | void |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Elimina una descripción de norma de emisión de certificados |
| **Parámetros** | policyInformation : RevocationList -- una referencia de la norma que hay que eliminar del sistema |
| **Expresiones de precondición** | Ninguno |
| **Expresiones de precondición (OCL)** | true |
| **Expresiones de postcondición** | **policy**: La información de la norma se elimina del sistema |
| **Expresiones de postcondición (OCL)** | **policy**: true |
| **Comentarios** | Ninguno |

### Validaciones

|  |  |
| --- | --- |
| **SOP-0017** | **EmailValidationStart** |
| **Tipo del resultado** | String |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Inicia la validación de una dirección de correo electrónico. Asocia a un usuario una dirección de correo y un código único que se debe enviar por email. |
| **Parámetros** | user : User -- el usuario que inicia la validación email : String -- la dirección de correo que se quiere validar |
| **Expresiones de precondición** | Ninguno |
| **Expresiones de precondición (OCL)** | true |
| **Expresiones de postcondición** | **code**: Se envía un código único a la dirección de correo electrónico |
| **Expresiones de postcondición (OCL)** | **code**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0018** | **EmailValidationComplete** |
| **Tipo del resultado** | Bool |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Termina la validación de una dirección de correo electrónico. Si el código que envía el usuario coincide con el almacenado en el sistema, entonces el usuario queda activado. |
| **Parámetros** | user : User -- el usuario que inicia la validación code : String -- código que el usuario ha recibido por correo electrónico |
| **Expresiones de precondición** | **user**: El usuario debe existir en el sistema |
| **Expresiones de precondición (OCL)** | **user**: true |
| **Expresiones de postcondición** | **user**: El usuario queda activado en el sistema |
| **Expresiones de postcondición (OCL)** | **user**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **EmailValidationComplete::ValueError** |
| **Condición** | El código enviado por el usuario no coincide con el almacenado por el sistema |
| **Condición (OCL)** | false |
| **Expresión** | La validación queda cancelada y el usuario queda inactivo. |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0019** | **DNSValidationStart** |
| **Tipo del resultado** | String |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Inicia la validación de un dominio DNS. El sistema crea un código único que el usuario debe incluir en un registro TXT del dominio DNS que quiere validar. |
| **Parámetros** | user : User -- el usuario que inicia la validación domain : String -- el nombre del dominio que se quiere validar |
| **Expresiones de precondición** | **user**: El usuario debe existir en el sistema y estar activo |
| **Expresiones de precondición (OCL)** | **user**: true |
| **Expresiones de postcondición** | **code**: Se asocia un código único al usuario y dominio y se devuelve el código para que el usuario lo añada en su dominio. |
| **Expresiones de postcondición (OCL)** | **code**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **DNSValidationStart::DomainNotFoundError** |
| **Condición** | El nombre del dominio no se puede resolver |
| **Condición (OCL)** | false |
| **Expresión** | El nombre del dominio debe ser un nombre de dominio público y accesible desde la CA |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **SOP-0020** | **DNSValidationComplete** |
| **Tipo del resultado** | Bool |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\Users\jesusfer\OneDrive\Universidad\webca-docs.git\rem\WebCA_REM_Default_Spanish_DRS.html#STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Completa la validación de un dominio DNS. Comprueba que el valor asociado al usuario y dominio existe en un registro TXT del dominio y coincide con el valor registrado. |
| **Parámetros** | user : User -- el usuario que inicia la validación domain : String -- el nombre del dominio que se quiere validar |
| **Expresiones de precondición** | **user**: El usuario debe existir en el sistema y estar activo **domain**: El usuario debe tener pendiente una validación del dominio |
| **Expresiones de precondición (OCL)** | **user**: true **domain**: true |
| **Expresiones de postcondición** | **domain**: El dominio queda validado y asociado con el usuario |
| **Expresiones de postcondición (OCL)** | **domain**: true |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **Excepción** | **DNSValidationComplete::DomainNotFoundError** |
| **Condición** | El nombre del dominio no se puede resolver |
| **Condición (OCL)** | false |
| **Expresión** | El nombre del dominio debe ser un nombre de dominio público y accesible desde la CA |
| **Expresión OCL** | true |
| **Comentarios** | Ninguno |

### Usuarios

|  |  |
| --- | --- |
| **SOP-0014** | **UpdateUser** |
| **Tipo del resultado** | User |
| **Versión** | 1.0 (18/05/2018) |
| **Autores** | * [Jesús Fernández](file:///C:\\Users\\jesusfer\\OneDrive\\Universidad\\webca-docs.git\\rem\\WebCA_REM_Default_Spanish_DRS.html" \l "STK-0001) |
| **Dependencias** | Ninguno |
| **Descripción** | Cambia las propiedades de un usuario |
| **Parámetros** | user : User -- el usuario que se quiere modificar groups : Set(Group) -- el conjunto de grupos a los que pertenece el usuario permissions : Set(Permission) -- el conjunto de permisos que el usuario debe tener en el sistema operator : Integer -- si el usuario es operador del sistema o no |
| **Expresiones de precondición** | **user**: El usuario debe existir en el sistema |
| **Expresiones de precondición (OCL)** | **user**: true |
| **Expresiones de postcondición** | **groups**: El usuario pertenece exclusivamente a los grupos que hay en 'groups' **permissions**: El usuario tendrá exclusivamente los permisos que aparecen en 'permissions' **operator**: Según el valor de 'operator' el usuario podrá acceder a la sección de administración del sistema |
| **Expresiones de postcondición (OCL)** | **groups**: true **permissions**: true **operator**: true |
| **Comentarios** | Ninguno |

# Diseño de arquitectura

En este epígrafe se desarrolla la arquitectura de la solución implementada, justificando el uso de las tecnologías usadas para el desarrollo del sistema.

## Tecnología usada

Para esta solución, hay al menos dos decisiones que tomar respecto a qué tecnologías elegir. Dado que se trata de proyecto software, la primera decisión es qué lenguaje de programación, ya que eso determinará en qué plataformas se podrá implementar la solución una vez esté terminada. Elegir el lenguaje de programación también determina qué framework usar para que la implementación de la solución sea más fácil por lo que, en la mayoría de los casos, es la elección del framework de desarrollo la que determina finalmente el lenguaje de programación. Ya que la solución propuesta es una aplicación web, hay lenguajes que vienen impuestos como HTML o JavaScript ya que son los que los navegadores web entienden. En este proyecto, la segunda decisión a tomar es qué librería de criptografía usar. Una librería de criptografía proporcionará una serie de funciones ya probadas para poder generar, entre otras cosas, números aleatorios, parejas de claves y realizar acciones de cifrado/descifrado o firma/verificación.

Para una aplicación web hay que distinguir entre la capa del servidor y la capa de presentación. La capa de servidor será la que procese las peticiones de los usuarios, además de conectarse a sistemas externos en caso de que hiciera falta. Por último, generará las respuestas a los usuarios que sus navegadores web renderizarán. Las respuestas serán por lo general una página web HTML y en algunos casos será una respuesta XML/JSON si se trata de un servicio web. La capa de presentación serán páginas web descritas en el lenguaje estándar HTML5 soportado por los navegadores actuales. Las páginas web también pueden incluir código JavaScript que se ejecuta en el navegador del cliente para así poder ayudar en la presentación del contenido o para realizar acciones dinámicas, como llamar a un servicio web o alterar el contenido de la página sin que el servidor participe en ello.

### Programación de la capa servidor

Para la capa de servidor, Python ha sido elegido como lenguaje de programación principal para este proyecto.

Según el índice de popularidad que se analice, Python suele estar en las primeras posiciones. Si se revisa el índice PYPL, que calcula sus resultados en base al número de veces que se busca en Google un tutorial para un lenguaje determinado de programación, Python aparece el primero[[16]](#footnote-17) respecto al año anterior (última estadística calculada en mayo de 2018). Según el índice Spectrum del IEEE, Python también fue el primero[[17]](#footnote-18) en la clasificación del año 2017. Este índice usa 12 métricas de 10 fuentes diferentes para calcular sus resultados. Por último, según RedMonk[[18]](#footnote-19), que mira la frecuencia de las etiquetas de cada lenguaje en Stack Overflow[[19]](#footnote-20) y el número de proyectos en Github[[20]](#footnote-21) que usan dicho lenguaje, calculan que Python sería el tercero de la clasificación.

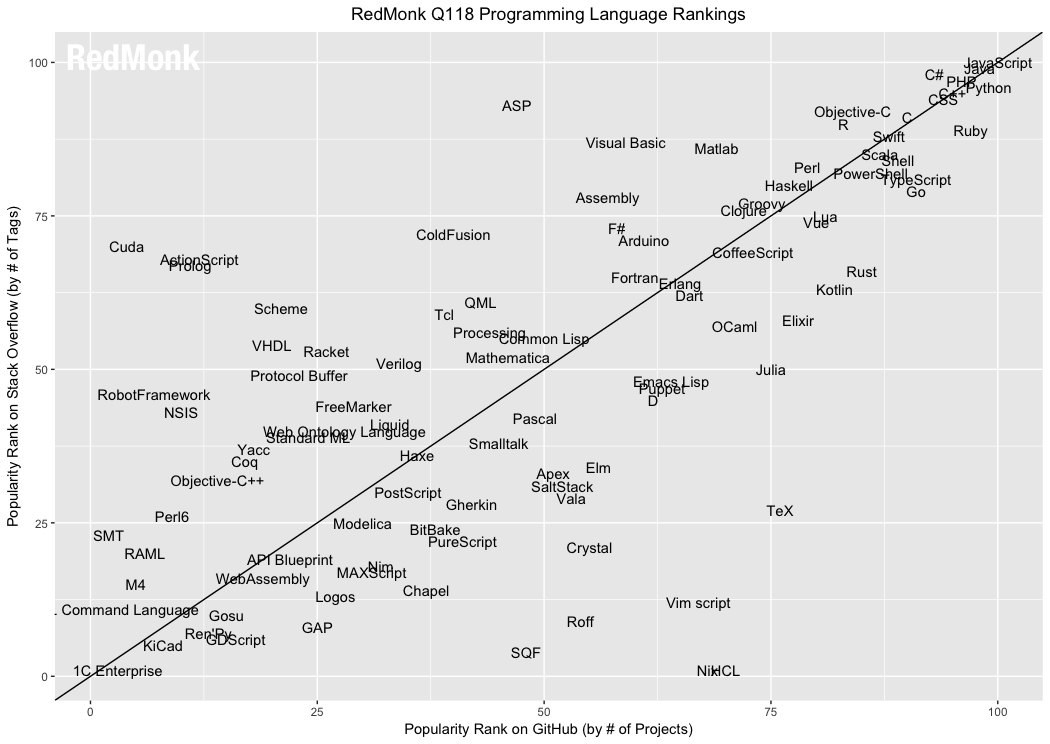


Ilustración 1. Clasificación de popularidad de los lenguajes de programación de RedMonk.

#### Django framework

Aunque Python parezca como uno de los lenguajes más populares del momento, esa no debe ser la única razón por la que se debe elegir un lenguaje de programación para un proyecto. En este caso, existe un framework de desarrollo web escrito en Python realmente interesante y que sí es la causa principal por la que se ha elegido Python. Este framework es Django[[21]](#footnote-22).

Django permite el desarrollo rápido y eficiente de aplicaciones web. Django usa una arquitectura parecida a Modelo-Vista-Controlador o MVC. Según la jerga de Django, se usa una arquitectura MTV, es decir, Modelo-Plantilla-Vista (T de *template* en inglés).

Un Modelo es una entidad que se necesita almacenar en base de datos. A nivel de base de datos, un modelo se representa con una tabla. En Python, un modelo es una clase con una serie de propiedades de diferentes tipos. Cada una de estas propiedades se traduce en una columna de la tabla. Además, se permiten diferentes tipos de relaciones entre modelos, con lo que se consigue relacionar tablas en la base de datos con las diferentes cardinalidades posibles, ya sean 1:1, 1:N, N:1 o N:M. Los modelos también guardan la integridad referencial a nivel de base de datos, incluso emulándola si el motor de la base de datos no la soporta.

Una Plantilla en Django es lo que determina cómo se le presenta al usuario uno o varios modelos.

Una Vista determina qué datos se le van a presentar al usuario, pero no cómo, ya que eso lo hace la plantilla. Las vistas también incorporan la lógica de negocio que se encargan de manipularlos datos entre modelos y usuario.

Por tanto, no se puede hacer una correlación entre Plantillas y Vistas con la Vista del modelo MVC porque en este último, la vista se encarga de determinar qué modelos y cómo se muestran al usuario y cómo interactúa el usuario con esos datos.

Tampoco existe como tal un controlador, aunque, según la propia explicación del modelo en la web de Django[[22]](#footnote-23), se podría considerar el controlador como el propio framework, ya que es el que se encarga de decidir qué vista corresponde con qué entrada y es el que orquesta todo el funcionamiento.

Por otra parte, Django proporciona una serie de características de caja muy interesantes:

* ORM, Object Relational Mapper. Un ORM es una abstracción de la capa de base de datos de manera que el programador no tiene que generar las consultas a las bases de datos manualmente. Las tablas de la base de datos se traducen en modelos/clases con propiedades y métodos que según sus valores generarán unas consultas u otras. Además, un ORM hace al programador que el acceso a la base de datos sea agnóstico del software que se ejecute en el servidor y así genere las consultas con las particularidades de cada motor. Django es compatible con diferentes motores de bases de datos como Oracle, MySQL, PostgreSQL o SQLite.
* Autenticación de usuarios. Incluido en el propio framework un mecanismo sencillo de autenticación de usuarios mediante usuario/contraseña, que es fácilmente extensible mediante la creación de *backends* para permitir otros tipos de autenticación.
* Sitio de administración automático. Incluye un sitio de administración que permite la administración de los modelos con todas las operaciones CRUD (creación, lectura, actualización y borrado), que además es fácilmente extensible para incorporar funcionalidades adicionales.
* Enrutado de vistas y URLs. La manera de crear y especificar URLs “bonitas” es tremendamente sencillo ya que permite la creación de URLs mediante expresiones regulares y asociarlas con las vistas fácilmente. Permite además asociar a cada URL o plantilla de URL un nombre y un espacio de nombres para poder referenciarlas desde el código sin tener que usar la URL real. De esta manera, si hace falta cambiar una URL, solo hay que cambiarla en un único sitio y no hace falta buscarla en todo el código fuente.
* La presentación de las respuestas se realiza mediante plantillas, que usan su propio lenguaje de etiquetas y filtros para incluir los datos que las vistas quieren representar. Las etiquetas realizan las funciones típicas de los lenguajes de programación para controlar el flujo como expresiones condicionales o bucles y los filtros permiten modificar la presentación de un dato determinado como, por ejemplo, convertir una cadena a mayúsculas o pintar un valor por defecto en caso de que un dato no tuviera valor. Por supuesto, se pueden crear nuevas etiquetas o filtros para modificar o representar los datos de alguna otra manera.
* Soporte a la localización y traducción de todo el contenido, tanto estático como dinámico, mediante el uso de librerías estándar. Se puede traducir tanto el contenido de las plantillas como cadenas de texto en el código de las vistas.

#### OpenSSL

Para las operaciones criptográficas, se elige OpenSSL como librería base de este proyecto. El principal motivo de esta elección es que es la principal librería criptográfica de código abierto y para la que existen múltiples adaptaciones para los diferentes lenguajes de programación. Por supuesto, OpenSSL cuenta con varias adaptaciones o bindings para Python. Como librería principal se usa *pyOpenSSL*[[23]](#footnote-24) ya que permite realizar la mayoría de las operaciones necesarias de una manera relativamente sencilla. A veces es una librería difícil de manejar debido al formato de los argumentos de entrada de sus funciones y a que los tipos de datos de entrada y salida no son homogéneos en ciertas partes de la API, pero resuelve la mayoría de las necesidades. Para aquellos casos en los que *pyOpenSSL* se queda corto, se usa la librería *cryptography*[[24]](#footnote-25). La propia librería pyOpenSSL proporciona métodos para convertir los tipos de datos entre ambas librerías, simplificando el proceso de un paso de una a otra. Es necesario usar cryptography, por ejemplo, para generar las listas de revocación de certificados, para trabajar con claves de curvas elípticas (EC) o para validar las firmas digitales que se usan en el protocolo de autenticación de la aplicación web.

Aun siendo Python y OpenSSL un lenguaje y una librería muy populares, los bindings de pyOpenSSL/cryptography e incluso la propia librería OpenSSL no permiten realizar ciertas operaciones como la creación de Delta CRL o listas de revocación incrementales.

Para el respondedor OCSP, ha hecho falta usar otra librería que soporta el procesamiento de las peticiones OCSP[[25]](#footnote-26) y la creación de respuestas OCSP[[26]](#footnote-27). Estas librerías también usan los bindings de OpenSSL.

### Programación de la capa cliente

Para esta capa no existe realmente una alternativa a HTML, JavaScript o CSS ya que este proyecto es una aplicación web y es HTML el estándar usado para describir páginas web. En este proyecto, la mayoría de las páginas son relativamente estáticas, por lo que, además de HTML se usa CSS para describir los estilos con los que el navegador debe renderizar cada elemento. Se ha intentado usar la mayor cantidad de atributos HTML5 para reducir la cantidad de código cliente JavaScript. Esto es realmente importante en la parte de los formularios web, donde siempre es conveniente intentar validar los datos antes de enviarlos al servidor. Así, usando los atributos de HTML5 adecuados, como required o estableciendo el tipo correcto de los elementos input, estas funciones de validación las realizar el propio navegador sin necesidad de escribir código. Por supuesto, una vez que los datos llegan al servidor son validados allí por la propia funcionalidad de Django y, en casos necesarios, por la validación realizada en el código del proyecto.

Donde el código JavaScript sí es muy importante es en el protocolo de autenticación mediante una pareja de claves asimétrica. Este protocolo será descrito más adelante, así como los detalles de su implementación. Para este protocolo, se ha hecho uso de la librería JavaScript habitual jQuery para ayudar con la llamada a servicios web, así como la librería de criptografía OpenCrypto[[27]](#footnote-28) para simplificar el uso de la API Web Crypto[[28]](#footnote-29) de los navegadores actuales.

## Arquitectura de la solución

TODO

### Componentes del sistema

La solución se compone de diferentes componentes: dos bases de datos, 3 aplicaciones web y un servicio. La seguridad es el motivo por el que existen varias bases de datos y varias aplicaciones web. Por una parte, se tienen dos aplicaciones web porque se quiere separar completamente la administración del sistema con el acceso de los usuarios. La tercera aplicación web es el respondedor OCSP. Respecto a las bases de datos, una de ellas es la que da servicio a la aplicación de los usuarios, por lo que almacena las solicitudes de firma, las plantillas y los certificados emitidos por la CA. La segunda base de datos se usa para almacenar las parejas de claves y los certificados usados por la CA para sus operaciones. Además, tener dos bases de datos diferentes permite configurar diferentes niveles de permisos a nivel de servidor de base de datos para que en caso de verse una comprometida, la otra no tenga que estarlo. El servicio es el que se encarga de emitir los certificados de los usuarios y de generar las listas de revocación según la programación.

Una de las ventajas de tener cada operación del sistema en diferentes componentes y de usar bases de datos es que cada servicio se puede desplegar en diferentes máquinas con lo que así también se aumenta la seguridad. Por ejemplo, una máquina puede ejecutar la web pública y desde esa máquina solo se puede acceder al servidor de bases de datos de la web pública. El servicio y la web de administración se pueden ejecutar desde otra máquina y esa ya sí tendría acceso a ambos servidores de BBDD. De esta manera, si se compromete la web pública, las claves de la CA no tienen por qué verse comprometidas. Igualmente, el servidor OCSP tiene su certificado de firma localmente y no accede a la base de datos de certificados, aunque sí es posible configurarlo para que obtenga el certificado de firma desde la base de datos.

El siguiente diagrama explica los diferentes componentes del sistema y cómo interactúan entre ellos.

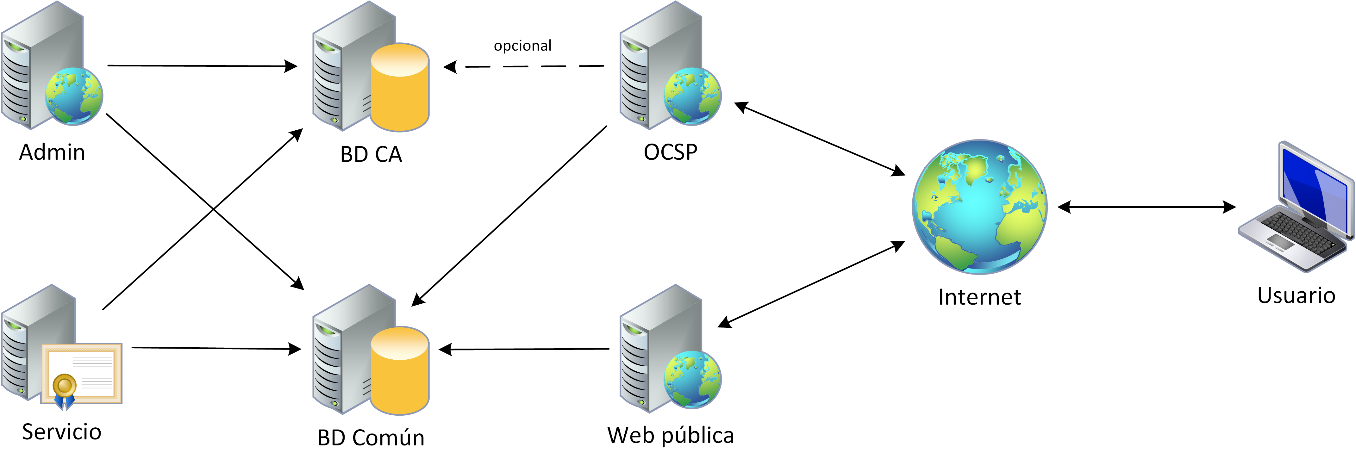


Figura 14. Arquitectura de la solución implementada

#### Web pública

* La web pública es la web a la que acceden los usuarios y donde realizan las solicitudes de emisión y revocación de certificados.
* Usa la base de datos predeterminada del sistema.
* No publica el sitio de administración.

#### Web de administración

* Sitio de administración del sistema que permite cambiar la configuración del sistema y controlar la emisión de los certificados: aprobar o revocar manualmente los certificados, administración de plantillas de certificados, cambiar los certificados usados por la CA, configurar la creación de CRLs, etc.
* Está basado en el sitio de administración que proporciona Django, con páginas adicionales para las acciones adicionales de administración.
* Accede a las dos bases de datos: web pública y almacén de certificados.

#### Servicio CA

* Servicio no interactivo que se ejecuta en modo daemon.
* Se encarga de revisar la lista de peticiones pendientes y emitir los certificados que estén aprobados para su emisión.
* Revisa también la lista de certificados revocados y crea una CRL completa según la configuración establecida.
* Accede a las dos bases de datos: web pública y almacén de certificados.
* Usa la clave privada de la CA para firmar los certificados emitidos y las CRL y usa un certificado propio para generar los CSR intermedios a la emisión de los certificados.

#### Respondedor OCSP

* Aplicación web pública y anónima que recibe solicitudes OCSP de clientes para comprobar la validez de los certificados.
* Accede a las dos bases de datos: web pública y almacén de certificados.
* Usa la clave privada del certificado OCSP.

### Certificados usados por el sistema

Del epígrafe anterior se entiende que existen varios certificados durante la ejecución de Web CA. El sistema necesita como mínimo 3 certificados con sus claves privadas para su correcto funcionamiento.

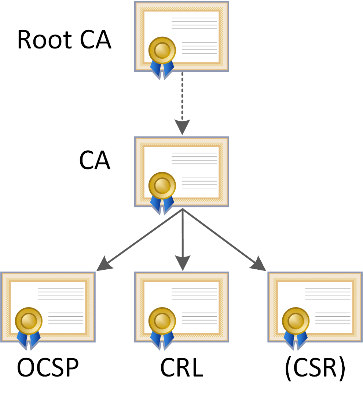


Figura 15. Certificados que usa Web CA para su funcionamiento

|  |  |
| --- | --- |
| Certificado CA | * Certificado principal. Es el que firma los certificados emitidos por la CA. * De manera predeterminada, firma también las CRL. |
| Certificado interno CSR | * A la hora de emitir los certificados, se crea un CSR intermedio con la clave pública del usuario y las extensiones de la plantilla. * Dado que este CSR tiene que estar firmado, se hace con este certificado intermedio. |
| Certificado OCSP | * Las respuestas OCSP deben estar firmadas por un certificado en el que la extensión ExtendedKeyUsage contiene OCSPSigning * Durante la configuración, el sistema genera un certificado tipo End Entity con la extensión ExtendedKeyUsage correcta firmado por el certificado de la CA |

Adicionalmente, se puede usar un certificado extra para firmar las CRL generadas por el sistema. Este certificado adicional se puede configurar en el sitio de administración. Igualmente, desde la administración se puede cambiar el certificado de la CA o el certificado OCSP en cualquier momento, previa instalación del nuevo.

La instalación de certificados nuevos se puede hacer mediante la web de administración (con PFX sin contraseña) o mediante un comando de administración de consola para PFX con contraseña.

### Procesos del sistema

En este epígrafe se detallan los procesos o casos de uso que involucran al usuario final y su interacción con el sistema.

#### Autenticación de los usuarios

La autenticación de los usuarios se puede hacer de dos maneras:

1. Mediante un código de un solo uso. Cuando el usuario quiere acceder al sistema, este crea un código de un solo uso que el usuario recibe por correo electrónico.
2. Mediante una pareja de claves criptográficas. Se genera una pareja de claves en el navegador del usuario y se usa una firma digital para confirmar la identidad.

##### Acceso mediante código de un solo uso

[Diagrama]

Figura 16. Flujo de la autenticación con un código de un solo uso

* El primer acceso es siempre mediante una dirección de correo electrónico. El usuario accede al sistema e introduce su dirección de correo electrónico.
* Si el sistema detecta que esta dirección de correo electrónico no se ha usado antes, entonces crea un registro para el usuario.
* El sistema crea un código de un único uso que envía al usuario a la dirección de correo electrónico y le solicita al usuario el código mediante la página web.
* Cuando el usuario recibe el correo electrónico, copia y pega el código en la página web y si coincide con el código que el sistema tiene almacenado, entonces le da acceso.

##### Acceso mediante una pareja de claves criptográficas

[Diagrama]

Figura 17. Flujo de la autenticación con claves criptográficas

1. Una vez que el usuario ha accedido al sistema por primera vez, se le da la opción de generar una pareja de claves en su navegador. Si el usuario decide configurar este método de autenticación se harán los siguientes pasos:
   * Haciendo uso de la API Web Crypto de los navegadores recientes, se genera una pareja de claves RSA de 2048 bits que se almacena en el propio navegador del usuario. Para almacenar las claves, se hace uso de IndexedDB[[29]](#footnote-30), una base de datos no relacional que permite almacenar una gran cantidad de información persistentemente. A la hora de almacenar la clave privada, se le solicita al usuario una contraseña para así poder guardar la clave cifrada.
   * Una vez que se tiene almacenada la pareja de claves, la clave pública se almacena en el servidor y se asocia con el usuario. Un usuario puede tener diferentes claves públicas.
   * La clave privada nunca sale del navegador del usuario.
2. Una vez que el navegador del usuario está configurado, ya puede hacer uso de este sistema de autenticación.
3. Cuando el usuario accede al sistema sin haber iniciado sesión, el sistema detecta si el usuario tiene alguna pareja de claves instalada. Si es así, muestra un formulario al usuario donde puede elegir la pareja de claves (si hubiera varias) y se le solicitará la contraseña usada para cifrar la clave privada.
4. Después de que el usuario elija la pareja de claves e introduzca la contraseña de la clave privada, se envía un mensaje al sistema. Este mensaje contiene dos partes: la dirección de correo del usuario con la que quiere iniciar sesión y un mensaje firmado por su clave privada. El mensaje firmado es la misma dirección de correo electrónico.
5. Cuando el sistema recibe el mensaje de autenticación, comprueba la validez de la firma con las claves públicas que conoce del usuario. Si alguna de las claves públicas valida la firma enviada, entonces se da acceso al usuario.

Hay que hacer notar que para que este proceso funcione es necesario que la comunicación entre el navegador y el servidor sea mediante HTTPS. Si no es así, y como medida de seguridad, los navegadores no permitirán el acceso a la API Web Crypto, por lo que no se podrá ni generar la pareja de claves ni manipular cualquiera que ya exista. Además, el almacenamiento está restringido a la URL que lo ha creado, por lo que solo se puede acceder desde código proporcionado por el sistema.

#### Emisión de certificados

[Gráfico del proceso de emisión de un certificado]

Figura 18. Proceso de emisión de un certificado

El proceso habitual que se utilizará para emitir certificados es el siguiente:

1. El usuario debe generar una pareja de claves y una solicitud de certificados en su propia máquina. Con esto debe obtener al menos dos archivos. Un archivo con su clave privada, habitualmente codificada en PKCS#8 y un archivo CSR codificado según PKCS#10.
2. El usuario accede al sistema y entra en la sección de solicitudes de certificado.
3. Se le muestra la lista de certificados que ya ha solicitado, así como un desplegable donde puede seleccionar un tipo de certificado. Un usuario no tiene por qué poder ver todas las plantillas que haya disponibles en el sistema. Solo puede ver aquellas en las que tiene permiso.
4. Cuando el usuario elige la plantilla, se le muestra una serie de campos que debe rellenar, como por ejemplo el nombre del certificado o una dirección de correo. También debe copiar y pegar el texto del CSR que debe haber generado previamente. Al enviar el CSR, el usuario está enviado la clave pública que se firmará al emitir el certificado.
5. Ahora, dependiendo de la configuración de la plantilla, el certificado se puede emitir automáticamente o puede hacer falta la aprobación de un operador.
6. Una vez que el certificado sea emitido, el usuario puede volver a la lista de solicitudes y desde ahí podrá descargar el certificado solicitado.

#### Revocación de un certificado

[Gráfico de la revocación de un certificado]

Figura 19. Proceso de revocación de un certificado

Por último, un usuario puede solicitar la revocación del certificado.

1. El usuario accede al sistema y elige la opción de revocar uno de sus certificados.
2. El sistema mostrará los certificados candidatos. Si un certificado ya está revocado o expirado, no se mostrará.
3. El usuario elige el certificado y también debe indicar el motivo de la revocación.
4. Una vez confirma que quiere realizar la acción, el sistema revoca inmediatamente el certificado.

## Patrones de diseño

Esta es una lista de algunos patrones de diseño de software que se usan o que se han implementado en este proyecto.

#### MVC

Como ya se explicó en el punto 8.1.1, el framework de desarrollo web Django usa un patrón similar al Modelo-Vista-Controlador, aunque denominado MTV según la propia documentación del proyecto.

#### Factoría Abstracta

Este patrón permite crear conjuntos de objetos de una misma familia. Mediante una clase abstracta, una serie de clases concretas implementarán una serie de métodos abstractos para devolver el mismo conjunto de tipos de resultado. De esta manera, el cliente usa una de las clases concretas sabiendo que obtendrá un objeto de una clase determinada, independientemente de cómo sea la implementación de la clase concreta y de los tipos que usen esas clases concretas.

El almacenamiento de las parejas de claves y certificados está planteado siguiendo este patrón. En este caso, se permite tener diferentes maneras de almacenar claves y certificados para su uso en la CA. Se define una clase abstracta CertStore que es el punto de entrada a todos los tipos diferentes de almacenes de certificados. Los diferentes almacenes implementan la clase CertStore, como por ejemplo la clase DatabaseStore e, independientemente de cómo DatabaseStore almacene los certificados, la clase que la consuma obtendrá siempre un tipo concreto de certificado, en este caso un objeto X509 de OpenSSL. En el caso de DatabaseStore, esta clase almacena los datos en modelos de Django, pero siempre devuelve un tipo determinado de la familia OpenSSL. Por ejemplo, si existiera una implementación FilesystemStore, esta podría almacenar la información en archivos, pero también devolvería objetos de la familia OpenSSL.

#### Fachada

El patrón Fachada permite reducir la complejidad del acceso a diferentes módulos, potencialmente uniendo las funcionalidades de diferentes módulos en uno solo.

Dado que ha sido necesario usar diferentes implementaciones y abstracciones de OpenSSL en este proyecto, se ha creado un módulo crypto que da un acceso menos complejo y más estándar a las partes interesantes de cada implementación. Este módulo implementa la mayoría de las operaciones criptográficas del sistema usando las funcionalidades de cada implementación según sea necesario. Esta fachada proporciona métodos sencillos como create\_key\_pair o create\_certificate y abstrae de las complejidades de la implementación que se usa.

#### Singleton

Este patrón garantiza la existencia de una única instancia de una clase y proporciona una manera de acceder a esa instancia única.

El código de autenticación de usuarios mediante claves hace uso de este patrón ya que el acceso a los métodos de IndexedDB y WebCrypto se hace mediante objetos singleton.

# Implementación

En este epígrafe se dan detalles de la implementación de la solución, herramientas usadas y resultados obtenidos.

## Entorno de desarrollo

Para escribir el código de la aplicación se ha usado Visual Studio Code[[30]](#footnote-31) sobre Microsoft Windows. VSCode no llega a ser un IDE al estilo de Eclipse o Visual Studio si no que es un sencillamente un editor de código fuente que soporta ciertos lenguajes de programación nativamente, tiene alguna capacidad de debugging y además tiene integrado el soporte para trabajar con sistemas de control de versiones. Además, cuenta con un sistema de extensiones que añaden funcionalidades en el editor. Para este proyecto se han usado varias, siendo las siguientes las principales:

* **Python**: da soporte al lenguaje Python en VSCode incluyendo funcionalidades de *linting*[[31]](#footnote-32), navegación del código, refactorización, etc.
* **Django Snippets**: ayuda en la creación de las plantillas HTML, sugiriendo etiquetas de Django.
* **guid**: proporciona un comando para generar UUID[[32]](#footnote-33) aleatorios.

Como repositorio de código y control de versiones se usa un repositorio Git[[33]](#footnote-34), proporcionado por GitHub (<https://github.com/jesusfer/webca>). Se ha elegido Git como control de versiones por ser un sistema muy flexible en la creación de diferentes ramas de desarrollo, pudiendo pasar de una a otra fácilmente. Además, permite crear ramas locales y hacer commits locales, sin necesidad de conectarse al repositorio principal. Se ha elegido GitHub para alojar el repositorio de código por ser gratuito, público y porque proporciona opciones para otros desarrolladores para interactuar con el código, reportar problemas o sugerencias. También es un servicio que aloja gran cantidad de proyectos de código abierto, como los propios Django u OpenSSL.

Para la organización de las tareas necesarias se ha usado Visual Studio Team Services, ya que permite fácilmente crear tareas principales, subtareas y agruparlas en iteraciones como en las metodologías ágiles, asignando fechas límites, tareas de mejora o bugs, etc.

## Resultados del proyecto

Se incluye en este apartado una descripción física del proyecto, así como algunas estadísticas de los archivos que se han creado, lenguajes de programación utilizados o detalles de las bases de datos.

### Estructura de la aplicación

El repositorio principal de la aplicación es un proyecto típico de Django. En un proyecto de Django, existe una carpeta principal que es la que contiene el módulo de configuración general y una carpeta por aplicación de Django. Una aplicación de Django es un módulo que define sus propios modelos, vistas y plantillas.

En este caso, hay carpetas/módulos extra que no son aplicaciones de Django, ya que no tienen necesidad de definir modelos o vistas.

|  |  |
| --- | --- |
| **Carpeta raíz del proyecto** |  |
|  | * certs: claves y certificados de ejemplo * setup: script de configuración del sistema * webca: carpeta con el código del sistema * manage.py: script de administración de Django * resto: scripts de ayuda para ejecutar las aplicaciones |
| **Carpeta principal webca** |  |
|  | * ca\_admin: aplicación de administración del sistema * ca\_ocsp: aplicación del respondedor OCSP * ca\_service: servicio CA. Emite certificados y CRLs * certstore: clase abstracta para definir almacenes de certificados CA * certstore\_db: implementación certstore usando modelos Django * config: aplicación de configuración genéricas * crypto: funciones criptográficas genéricas * utils: funciones de utilidad * web: aplicación de la web pública * resto: archivos de configuración generales |

### Estadísticas de creación

Estas estadísticas incluyen el número de archivos que se han creado, líneas de código escritas, etc. Los datos se han obtenido usando la aplicación cloc[[34]](#footnote-35)que analiza los archivos del proyecto, identificando el lenguaje de cada uno de ellos y extrayendo métricas por cada línea.

En la siguiente tabla se puede ver el número de archivos creados según el lenguaje de programación. Como se puede ver, el número de archivos no es excesivamente elevado, por lo que eso nos puede dar una idea de las facilidades que proporciona Django para hacer una aplicación web funcional con relativamente pocos archivos de código.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Python** | **HTML** | **PowerShell** | **JavaScript** | **JSON** | **CSS** |
| **Número de archivos** | 101 | 26 | 4 | 3 | 2 | 1 |

Tabla 2. Número de archivos por lenguaje de programación

Respecto a la cantidad de código escrito, se muestra un gráfico con el número de líneas por lenguaje de programación utilizado. A diferencia de lo que ocurre con otros lenguajes de programación donde la cantidad de líneas efectivas de código que se escriben se ve incrementada por el uso de líneas que solo contienen signos de llaves para delimitar bloques de código, en Python no ocurre lo mismo ya que la delimitación de bloques se hace según la sangría de las líneas. Esto hace que en Python cada línea escrita sea efectiva y, además, ayude a un código más limpio.

Figura 20. Número de líneas de código por lenguaje

Por otra parte, otra medida que puede resultar interesante es la cantidad de líneas de comentarios por cada línea de código. La inclusión de comentarios en un proyecto es vital para que otros desarrolladores puedan entender más fácilmente partes del código que no puedan quedar claras a primera vista. Haciendo un cálculo de cuántas líneas de código hay por cada línea de comentario, para Python se tiene que hay una línea de comentario por cada 4 de código y para JavaScript la razón es de 1 línea de comentario por cada 20 de código.

Los números anteriores dan una idea de la cantidad de código que se ha escrito para el proyecto, pero para tener una idea de todo el código que compone el proyecto en general, se muestran en la siguiente tabla los números contando con el propio framework y todas las bibliotecas que se han usado.

TODO

## Bases de datos

Toda aplicación web que almacena datos necesita por lo general una base de datos. WebCA necesita dos bases de datos diferentes: una para el contenido de la web pública y otra para almacenar las claves y certificados usados para emitir los certificados de los usuarios.

Si bien es cierto que se podría usar una única base de datos, lo conveniente es que usar dos para así poder separar el acceso al contenido y el acceso a la parte más sensible que son las claves privadas de una CA. El sistema está desarrollado para que la aplicación web pública no necesite en ningún momento acceso a las claves privadas y así se reduzca el riesgo de comprometerlas.

Una de las ventajas de usar Django es que el desarrollador codifica los modelos en Python y es Django el que se encarga de crear las tablas e índices en las bases de datos. Esto también permite que el desarrollador no necesite saber a priori qué motor de base de datos se va a usar y así escribir código agnóstico a cualquier motor. Django dispone también de un sistema de detección de cambios en los modelos que se crean y para luego después poder aplicar esos cambios también en las bases de datos si es que ya están creadas. Esto permite añadir, modificar o quitar columnas en las bases de datos sin tener que modificarlas manualmente.

Dado que no hay estructuras excesivamente complejas en este proyecto no ha hecho falta cambiar o modificar las estructuras que Django genera en la base de datos. Únicamente se ha creado un índice en la tabla que guarda los certificados emitidos para así optimizar las búsquedas de certificados según el número de serie.

Habitualmente, la correspondencia entre modelos y tablas es uno a uno, es decir, por cada modelo que se define en Django, se crea una tabla en base de datos. Se pueden crear tablas adicionales si se definen relaciones del tipo varios a varios entre modelos. Por ejemplo, la tabla web\_template\_allowed\_groups, que almacena la relación entre plantillas de certificados y grupos de usuarios que tienen permitido usar las plantillas, es de este tipo.

En el gráfico siguiente se puede ver la relación entre las tablas de la base de datos de la web pública.

[Gráfico Entidad-Relación]

Figura 21. Modelos y relaciones de la base de datos de la web pública

## Ejemplos del código desarrollado

Se detallan algunas partes del código que pueden ser interesantes.

### Autenticación de usuarios

Una de las partes interesantes es la autenticación de los usuarios usando claves privadas. La función doLogin crea el mensaje firmado y lo envía al servicio web. Esta función demuestra el uso de la API Web Crypto mediante OpenCrypto[[35]](#footnote-36), así como también muestra el uso de los objetos Promise[[36]](#footnote-37) de JavaScript para operaciones asíncronas y las funciones flecha de ECMAScript 6[[37]](#footnote-38).

function doLogin(email, key) {

const crypto = new OpenCrypto();

var message = crypto.stringToArrayBuffer(email);

return window.crypto.subtle.sign(

{

name: "RSASSA-PKCS1-v1\_5",

hash: { name: "SHA-512" },

},

key,

message,

)

.catch(error => {

output("Couldn't create the signed message");

})

.then(signed => {

const crypto = new OpenCrypto();

const base64 = crypto.arrayBufferToBase64(signed);

return $.post('', {'email':email, 'signed':base64})

}) // Login errors are handled in the parent function

}

### Modelos del sistema

Como ejemplo de lo sencillo que resulta crear un modelo en Django, tenemos la clase KeyPair que almacena claves privadas y públicas. Esta clase se traduce en una tabla con 5 columnas: una columna *Id* autoincremental y 4 columnas para los 4 *Fields* de la clase.

class KeyPair(models.Model):

"""Represents a key pair that can be either RSA or DSA."""

name = models.CharField(

max\_length=255,

help\_text='Display name for this key pair',

)

private\_key = models.TextField(

default='',

help\_text='Private key in PEM format',

)

public\_key = models.TextField(

blank=True,

help\_text='Public key in PEM format. Might be blank.',

)

key\_type = models.IntegerField(

choices=dict\_as\_tuples(c.KEY\_TYPE),

default=c.KEY\_RSA,

)

### Respondedor OCSP

Finalmente, con estas seis líneas se genera una respuesta OCSP para un certificado revocado desde un modelo de Django (revoked) hasta una respuesta ASN.1:

der = crypto\_utils.export\_certificate(revoked.certificate.get\_certificate())

subject\_cert = asymmetric.load\_certificate(der)

revocation\_date = revoked.date

reason = REASONS[revoked.reason]

builder = OCSPResponseBuilder('successful', subject\_cert, reason, revocation\_date)

# Pruebas

Comprobar que los cambios que se hacen en el código no afectan al funcionamiento esperado del sistema es un proceso que debería ser natural para cualquier desarrollador. Una manera de comprobar que todo funciona después de realizar cambios en el código es tener una serie de acciones que realizar después de cada cambio. Cuando se detecte algún error en alguno de estos pasos, entonces se habrá introducido una regresión en el código en los cambios que se han hecho. Tener estos pasos bien detallados para poder identificar fácilmente qué parte del código están probando es clave para poder identificar fácilmente en qué parte del código se ha introducido la regresión.

La realización de estos pasos se puede hacer de manera manual, por ejemplo, teniendo una lista de cosas que hay que probar, en la que la persona que vaya a hacer las pruebas pueda ir marcando qué ha funcionado y qué no funciona ya.

## Pruebas unitarias

Aunque la estrategia anterior puede ser válida en proyectos pequeños o sencillos donde no haya una gran cantidad de casos que probar, en general es una estrategia anticuada. La mayoría de los lenguajes de programación permiten la creación de pruebas unitarias. Este tipo de pruebas consisten en crear más código que permite probar el código de una aplicación. La idea de una de estas pruebas es que se enfoque en una parte determinada del código, como una función o método de una clase. De esta manera, cuando esa prueba falle, se sabrá qué función es la que no funciona en el código del sistema. Por cada función o método se suelen crear varias pruebas, de manera que se prueben todas las combinaciones de los argumentos de entrada, de salida o incluso de las excepciones que se puedan lanzar. La idea básica es que la ejecución de las pruebas debe ejecutar todas las líneas de código de una función. También se pueden usar para simular las reglas de negocio, de manera que las diferentes combinaciones de argumentos de entrada sean adecuadas.

Un punto importante sobre las pruebas unitarias es que la persona que las escriba debería ser diferente a la persona que desarrolle el código. De esa manera, las pruebas se escriben sin tener en cuenta la implementación que se pueda hacer en el código y así son flexibles en caso que el código del método a probar cambie radicalmente.

Cuando se trabaja en equipos que comparten código fuente en repositorios de código, es relativamente habitual que cuando un desarrollador vaya a guardar los cambios que ha hecho en el repositorio, se lance la batería de pruebas. Según los resultados de las pruebas, se le permitirá guardar los cambios en el repositorio o no.

## Cobertura del código

Una métrica que se puede extraer de la ejecución de las pruebas unitarias es el porcentaje de código que está cubierto por una prueba, es decir, el porcentaje de código que es ejecutado durante la ejecución de las pruebas unitarias. Aunque podría parecer que la cobertura debería ser siempre del 100%, hay que tener en cuenta que se suelen tener en cuenta todas las líneas de código y que no todas ellas tienen por qué tener una prueba asociada. Por ejemplo, dentro de una clase se puede tener una propiedad que sencillamente devuelve un valor, sin tener que hacer un cálculo. Las líneas de esta propiedad se tendrán en cuenta para el cálculo de la cobertura, pero lo más probable es que nunca haga falta hacer una prueba para esa propiedad. De esta manera, la cobertura nunca será del 100%.

Tener un bajo porcentaje de cobertura quiere decir que el código no está suficientemente probado, mientras que un porcentaje alto no quiere decir que está bien probado. Para decir que un código está bien probado hay que tener en cuenta la calidad de las pruebas unitarias, no la cantidad de código que estas cubran.

## Testeo en Web CA

Se han desarrollado pruebas unitarias para el módulo de criptografía crypto, dado que es el que incluyen las funciones es vital que funcione siempre tal y como se necesita. Es por esto que el 100% del módulo está cubierto por pruebas unitarias. También es interesante cubrir las vistas de cara a los usuarios, como la web pública o el respondedor OCSP ya que eso permitiría validar que las entradas y las salidas son las que se esperan y, sobre todo, cómo se comporta el código con entradas inesperadas. El proyecto incluye pruebas unitarias para el respondedor OCSP.

Django extiende las funcionalidades del módulo nativo de Python unittest añadiendo funciones de comprobación para objetos de Django. Además, incluye un cliente para simular peticiones HTTP a las vistas de Django.

Además de la funcionalidad de Python y Django, se ha usado coverage.py[[38]](#footnote-39) para calcular la cobertura del código y codecov[[39]](#footnote-40) para obtener estadísticas y gráficos sobre la cobertura. El porcentaje de código cubierto está actualmente en 56%.

En el siguiente gráfico se puede ver en un gráfico radial la cobertura de código del proyecto. Las zonas verdes indican una alta cobertura y las zonas rojas indican una baja cobertura. En particular, la zona ocre en la parte superior se corresponde con el respondedor OCSP y la zona verde en la parte inferior es el módulo crypto del proyecto.

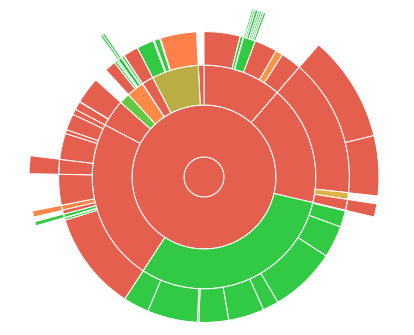


Figura . Cobertura de código realizado por codecov.

# Conclusiones y trabajos futuros

Se han cumplido los principales objetivos de este proyecto:

* Disponer de diferentes plantillas que especifican las características de los certificados que se van a emitir.
* Emitir certificados digitales en base a las mencionadas plantillas.
* Crear listas de revocación para comprobar la validez de los certificados emitidos
* Responder a preguntas OCSP para comprobar la validez de los certificados emitidos

Por tanto, una autoridad de certificación basada en Web CA cumple los requisitos mínimos para poder emitir certificados digitales.

Una de las dificultades encontradas durante la implementación del proyecto ha sido que OpenSSL aún no soporta la creación de listas de revocación incrementales o Delta CRL. Este tipo de listas se pueden generar entre la publicación de una CRL completa y otra y evitan que un sistema que quiera comprobar la validez de un certificado tenga que descargar una CRL completa. Una posibilidad para dotar a Web CA de la habilidad de generar Delta CRLs sería utilizar otra librería para generarlas, igual que se ha necesitado para el respondedor OCSP. Aun así, el sistema está preparado para soportar Delta CRL, pero se han dejado desactivadas esas opciones.

Otra dificultad que ha surgido y que ha provocado un cambio importante ha sido la autenticación de los usuarios. Según el plan inicial, la CA emitiría un certificado digital a cada usuario y así los usuarios usarían este certificado digital de usuario para autenticarse en el sistema. Es un método relativamente estándar cuando se trata de un escenario empresarial donde es fácil generar y distribuir estos certificados a los usuarios. Pero al tratarse Web CA de un software que no tiene por qué ser usado solo en un entorno empresarial, la generación del certificado de usuario causa problemas. El primero es que el usuario debe generar él mismo la clave privada y solicitar el certificado a la CA, tal y como se hace con cualquier otro certificado. Este escenario manual no es cómodo para el usuario. Por otra parte, antes era posible generar una pareja de claves en el mismo navegador y generar un certificado en el servidor e instalarlo en el navegador del usuario. El soporte a los elementos HTML necesarios para que esto funcionara se ha visto perjudicado con el nacimiento de la API Web Crypto. De hecho, esta API surge para estandarizar esos mismos elementos que se han desactivado. Aún hay navegadores que permiten usar estos elementos, pero dado que no es una solución que se pueda aplicar a la mayoría de los usuarios, no se ha dado por buena.

Así, se ha tenido que pensar en un nuevo protocolo de autenticación para los usuarios que permitiera autenticar a los usuarios de una manera más o menos automática y así nace la autenticación mediante claves. Ahora no se puede instalar un certificado en el navegador del usuario, pero sí se pueden generar parejas de claves con la nueva API y guardarlas en el navegador de manera que solo el código de la página que las ha generado pueda acceder a ellas. También se puede guardar la clave privada cifrada con una contraseña, para así limitar su acceso.

Como mejoras para el futuro, sería interesante que el sistema tuviera un flujo de trabajo para comprobar de una manera más o menos automática los datos de los usuarios y de los certificados que solicitan. Por ejemplo, sería interesante indicar en una plantilla que se debe hacer una comprobación de la validez real de una dirección de correo electrónico o de un dominio DNS.

Otra opción interesante es que un autor de plantillas de certificados pudiera incluir más extensiones de las que se incluyen de manera predeterminada. El sistema está preparado para poder especificar extensiones mediante una notación JSON y convertir este JSON en extensiones X509. Falta documentación e incluir estas extensiones personalizadas en los certificados emitidos. Sería necesario también crear algún tipo de precedencia para que una extensión personalizada no pueda sobrescribir lo que especifique la plantilla.

Un aspecto interesante que no se ha incluido en el proyecto es la creación de las normas de emisión de certificados. Esto se representa con la extensión *Certificate Policies* e indica una ruta desde donde descargar la documentación que indica los usos de los certificados emitidos por una CA, así como las reglas que esa CA sigue para emitir sus certificados. Es una manera de que un usuario entienda cómo funciona una determinada CA y sus procesos.

Finalmente, sería interesante seguir creando pruebas unitarias para aumentar la cobertura del código y poder testear partes como la emisión de certificados o las vistas de administración para importar o generar certificados.

# Bibliografía

|  |  |
| --- | --- |
| [1] | A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996. |
| [2] | RSA Laboratories, «Public-Key Cryptography Standards (PKCS),» [En línea]. Available: https://web.archive.org/web/20170417085550/https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm. [Último acceso: Enero 2018]. |
| [3] | ITU-T, «Abstract Syntax Notation One (ASN.1) Recommendations,» [En línea]. Available: https://www.itu.int/ITU-T/studygroups/com17/languages/. [Último acceso: Enero 2018]. |
| [4] | «Características Chip DNIe,» [En línea]. Available: https://www.dnielectronico.es/PortalDNIe/PRF1\_Cons02.action?pag=REF\_240&id\_menu=[26\_%2030]. [Último acceso: December 2017]. |
| [5] | ITU-T, «RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,» [En línea]. Available: https://tools.ietf.org/html/rfc5280. [Último acceso: Enero 2018]. |
| [6] | ITU-T, «RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,» [En línea]. Available: https://tools.ietf.org/html/rfc3280. [Último acceso: Enero 2018]. |
| [7] | ITU-T, «RFC 6818: Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,» [En línea]. Available: https://tools.ietf.org/html/rfc6818. [Último acceso: Enero 2018]. |
| [8] | ITU-T, «Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER),» [En línea]. Available: http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf. [Último acceso: Enero 2018]. |
| [9] | Oracle, «Sun Directory Server Enterprise Edition 7.0 Reference: Verifying a Certificate Chain,» [En línea]. Available: https://docs.oracle.com/cd/E19424-01/820-4811/gdzea/index.html. [Último acceso: Enero 2018]. |
| [10] | PKI Forum, «Understanding Certification Path Construction,» [En línea]. Available: http://www.oasis-pki.org/pdfs/Understanding\_Path\_construction-DS2.pdf. |
| [11] | ITU-T, «RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,» [En línea]. Available: https://tools.ietf.org/html/rfc6960. |
| [12] | ITU-T, «RFC 6066: Transport Layer Security (TLS) Extensions: Extension Definitions,» [En línea]. Available: https://tools.ietf.org/html/rfc6066. |
| [13] | ITU-T, «RFC 6961: The Transport Layer Security (TLS) Multiple Certificate Status Request Extension,» [En línea]. Available: https://tools.ietf.org/html/rfc6961. |
| [14] | RSA Laboratories, «RFC 2986: PKCS #10: Certification Request Syntax Specification Version 1.7,» [En línea]. Available: https://tools.ietf.org/html/rfc2986. [Último acceso: Marzo 2018]. |
| [15] | RSA Laboratories, «RFC 2985: PKCS #9: Selected Object Classes and Attribute Types Version 2.0,» [En línea]. Available: https://tools.ietf.org/html/rfc2985. [Último acceso: Marzo 2018]. |
| [16] | Certicom Corp, «Certicom Announces Elliptic Curve Cryptography Challenge Winner,» [En línea]. Available: https://web.archive.org/web/20110719233751/https://www.certicom.com/index.php/2004-press-releases/36-2004-press-releases/300-solution-required-team-of-mathematicians-2600-computers-and-17-months-. [Último acceso: Enero 2018]. |
| [17] | National Institute of Standards and Technology, «Recommendation for Key Management, Part 1: General,» [En línea]. Available: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final. |

1. CC o Common Criteria es una estándar ISO (ISO/IEC 15408) de certificación de seguridad informática. PP es el perfil de certificación Protection Profile y EAL significa Evaluation Assurance Level, la nota que se le otorga, que va desde 1 a 7, siendo 7 la mayor. [↑](#footnote-ref-2)
2. RFC 4086: Randomness Requirements for Security <http://tools.ietf.org/html/rfc4086> [↑](#footnote-ref-3)
3. PKCS #1: RSA Cryptography Specifications Version 2.2: <https://tools.ietf.org/html/rfc8017> [Accedido enero 2018] [↑](#footnote-ref-4)
4. Factorization of a 768-bit RSA modulus: Cryptology ePrint Archive: Report 2010/006: <https://ia.cr/2010/006> [Accedido enero 2018] [↑](#footnote-ref-5)
5. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms: IEEE Transactions on Information Theory, Vol 31, Julio 1985: <http://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf> [Accedido enero 2018] [↑](#footnote-ref-6)
6. What’s Elgamal?: <https://www.gnupg.org/faq/gnupg-faq.html#define_elgamal> [Accedido enero 2018] [↑](#footnote-ref-7)
7. FIPS 186-4: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf> [Accedido enero 2018] [↑](#footnote-ref-8)
8. Recommendation for Key Management, Part 1: General [17] [↑](#footnote-ref-9)
9. Certicom Announces Elliptic Curve Cryptography Challenge Winner [16] [↑](#footnote-ref-10)
10. Traducción de Cross-Validation Diagram. Wikipedia: <https://commons.wikimedia.org/wiki/File:Cross-certification_diagram.svg> [Accedido febrero 2018] [↑](#footnote-ref-11)
11. Manual Solicitud Certificado Persona Física. FNMT-Ceres. <https://www.cert.fnmt.es> [Accedido marzo 2018] [↑](#footnote-ref-12)
12. W3C. Especificación HTML 5.2: <https://www.w3.org/TR/html52/changes.html#features-removed> [Accedido marzo 2018] [↑](#footnote-ref-13)
13. SPKAC format for Certificate Signing Request (CSR): <https://github.com/jas-/node-spkac> [Accedido marzo 2018] [↑](#footnote-ref-14)
14. OpenSSL. Manual de spkac: <https://www.openssl.org/docs/manmaster/man1/spkac.html> [Accedido marzo 2018] [↑](#footnote-ref-15)
15. CA/Browser Forum. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates: <https://cabforum.org/baseline-requirements-documents/> [Accedido marzo 2018] [↑](#footnote-ref-16)
16. Índice PYPL: <http://pypl.github.io/PYPL.html> [↑](#footnote-ref-17)
17. Índice Spectrum: <https://spectrum.ieee.org/computing/software/the-2017-top-programming-languages> [↑](#footnote-ref-18)
18. RedMonk: <http://redmonk.com/sogrady/2018/03/07/language-rankings-1-18/> [↑](#footnote-ref-19)
19. Comunidad de desarrolladores Stack Overflow: https://stackoverflow.com [↑](#footnote-ref-20)
20. Comunidad de desarroladores y repositorios Github: <https://github.com> [↑](#footnote-ref-21)
21. Django Project: <https://www.djangoproject.com> [↑](#footnote-ref-22)
22. Django parece ser un framework MVC, pero ustedes llaman al Controlador «vista», y a la Vista «plantilla». ¿Cómo es que no usan los nombres estándares? <https://docs.djangoproject.com/es/2.0/faq/general/> [↑](#footnote-ref-23)
23. Documentación de pyOpenSSL: <https://pyopenssl.org/en/stable/> [↑](#footnote-ref-24)
24. Documentación de cryptography: <https://cryptography.io/> [↑](#footnote-ref-25)
25. Librería asn1crypto: <https://github.com/wbond/asn1crypto> [↑](#footnote-ref-26)
26. Librería ocspbuilder: https://github.com/wbond/ocspbuilder [↑](#footnote-ref-27)
27. Librería OpenCrypto para Javascript: <https://github.com/safebash/opencrypto> [↑](#footnote-ref-28)
28. API Web Crypto en MDN Web Docs: <https://developer.mozilla.org/es/docs/Web/API/Web_Crypto_API> [↑](#footnote-ref-29)
29. Descripción de IndexedDB: <https://developer.mozilla.org/en-US/docs/Web/API/IndexedDB_API> [↑](#footnote-ref-30)
30. Visual Studio Code: [https://code.visualstudio.com](https://code.visualstudio.com/) [↑](#footnote-ref-31)
31. Linting: Comprobar que el estilo del código es correcto: uso de tabuladores, nombres de variables, etc [↑](#footnote-ref-32)
32. Identificador único universal: <https://es.wikipedia.org/wiki/Identificador_%C3%BAnico_universal> [↑](#footnote-ref-33)
33. Git SCM: [https://git-scm.com](https://git-scm.com/) [↑](#footnote-ref-34)
34. Count lines of code: <http://github.com/AlDanial/cloc> [↑](#footnote-ref-35)
35. OpenCrypto: https://github.com/safebash/opencrypto [↑](#footnote-ref-36)
36. Promise object: https://developer.mozilla.org/en/docs/Web/JavaScript/Reference/Global\_Objects/Promise [↑](#footnote-ref-37)
37. Funciones flecha: https://hacks.mozilla.org/2015/06/es6-in-depth-arrow-functions/ [↑](#footnote-ref-38)
38. Coverage.py: <https://coverage.readthedocs.io> [↑](#footnote-ref-39)
39. Codecov: <https://codecov.io> [↑](#footnote-ref-40)