Contrato 53/2019

Canal de Isabel II

Pliego de Prescripciones Técnicas Particulares para la adquisición de certificados SSL para dominios Internet corporativos

Madrid, marzo de 2019

Área Infraestructura Informática

Índice

1. INTRODUCCIÓN

Canal de Isabel II S.A. utiliza en la actualidad certificados SSL Digicert (antes Symantec) para soportar las aplicaciones Web seguras que pública en Internet, correspondientes a los dominios 'canaldeisabelsegunda.es.es, 'cyii.es' y 'canalcaceres.es'. Los certificados para estos dominios se generan o renuevan con vigencia anual. siendo necesaria la adquisición de nuevos certificados SSL soportados bajo estos dominios.

Se identifican hoy en día un total de 19 certificados activos.

ep.canaldeisabelsegunda.es
mv.canaldeisabelsegunda.es
pm.canaldeisabelsegunda.es
riegoeficiente.canaldeisabelsegunda.es
mbc.canaldeisabelsegunda.es
oficinavirtual.canalcaceres.es
pcyiisred01.canaldeisabelsegunda.es
pre.canaldeisabelsegunda.es
licitaciones.canaldeisabelsegunda.es
pasarelapago.canaldeisabelsegunda.es
oficinavirtual.canaldeisabelsegunda.es
www.canaldeisabelsegunda.es
slc.canaldeisabelsegunda.es
srm.canaldeisabelsegunda.es
abyspa.canaldeisabelsegunda.es
www.cyii.es
acceso.canaldeisabelsegunda.es
movilidad.canaldeisabelsegunda.es
apl.canaldeisabelsegunda.es

Y se pretende dotar el contrato para cubrir ampliaciones futuras hasta un máximo de 25 certificados.

A efectos de simplificar y optimizar la gestión de estos certificados se contempla un contrato de duración de 3 años que permita manejar el ciclo de vida del conjunto de certificados por este periodo de 3 años superior al que hasta ahora se venía gestionando por un año. El planteamiento contemplado se valora bajo la posibilidad de gestionar un pool de certificados en modo suscripción, de cara a proporcionar la ventaja en relación a que la potencial baja de un certificado por desuso del dominio en cuestión en un momento determinado del contrato, se pueda reabsorber y reutilizar para otro potencial nuevo dominio, de tal forma que esta suscripción de certificado no se pierda.

A la par se pretende tener la posibilidad durante el ciclo de vida del contrato de poder adquirir certificados de tipo Wildcard (válidos para todos los nombres de un dominio completo), Multidomain (válidos para 4 o más nombres de dominio), EV (certificados de Validación Extendida) y SAN (nombres adicionales sobre los 4 contemplados de inicio en los Multidomain), de tal forma que el inventario estimado a cubrir en los 3 años de vida del contrato es el que sigue:

Tipo Certificado	Unidades
Certificado SSL	25
Certificado SSL Extended Validation	1
Certificado SSL Wildcard	1
Certificado SSL Multidomain	1
SAN Adicional Multidomain	2
SAN Adicional Multidomain EV	2

Las características particulares de cada tipo de certificado se especifican más adelante en el apartado de características técnicas y requerimientos.

2. ALCANCE

El objetivo de esta contratación es disponer de un servicio adquisición de certificados SSL que cubra el inventario estimado especificado con anterioridad, durante un período de vida de 3 años. Se establece así el siguiente escenario máximo hipotético de adquisición:

Tipo Certificado	Unidades
Certificado SSL	25
Certificado SSL Extended Validation	1
Certificado SSL Wildcard	1
Certificado SSL Multidomain	1
SAN Adicional Multidomain	2
SAN Adicional Multidomain EV	2

Quedando a discreción de Canal de Isabel II S.A la adquisición de los certificados que requiera en función de las necesidades que surjan durante el período de vida del contrato.

Quedan incluidos dentro del alcance del contrato certificados para las empresas/organismos:

- Ente Público Canal de Isabel II
- Canal de Isabel II, S.A.

Este servicio debe contemplar la puesta a disposición de una herramienta única de administración que permita la autonomía en la gestión de solicitudes, emisiones de certificados, revocaciones, en definitiva la gestión del ciclo de vida de los certificados.

La solución debe contemplar al menos un mínimo de 10 organizaciones, 10 dominios y 10 administradores.

Los certificados se podrán adquirir bajo demanda de forma unitaria y durante el período de vida del contrato de 3 años y se establecerá para todos ellos su caducidad, en el momento de adquisición, a fecha fin del período de contrato. En este escenario se plantea por tanto una duración variable igual o inferior a 3 años para cada uno de los certificados solicitados, que dependerá del momento en el que se adquiera la unidad de certificado, con lo que el coste se deberá ajustar de manera lineal y prorrateada al coste unitario establecido para los 3 años de duración en el momento de adquisición de cada certificado.

Se establece un modelo de suscripción de unidades de certificado en el que se pueda recuperar el derecho de uso de un certificado que potencialmente pudiera quedar obsoleta y quisiera darse de baja. En este sentido la baja de un certificado dominio asociado deja de dar servicio, no debe suponer la pérdida del derecho de uso de dicha unidad de certificado, esto es, dicho derecho adquirido debe poder reutilizarse para el alta de otro certificado con misma fecha de caducidad que el que se ha dado de baja.

Igualmente se contempla asociado al servicio de adquisición, un servicio de soporte avanzado con un mínimo de atención en 8x5.

Tanto los tipos de certificados arriba contemplados, los requisitos de la solución y del soporte requerido se detallan en el apartado de características técnicas.

3. CARACTERÍSTICAS TÉCNICAS

Se especifican a continuación las características técnicas mínimas que la solución debe contemplar.

3.1. Tipos de certificado

La solución ha de contemplar, al menos, la gestión y emisión de los siguientes tipos de certificado.

Tipo Certificado	Descripción
Certificado SSL	Asegura al menos dos dominios Asegura tanto el dominio www.dominio.com como dominio.com por defecto Algoritmos de hash: SHA-2 y ECC Número ilimitado de licencias de servidor Número ilimitado de reemisiones Validación de organización Tiempo de vida de hasta 825 días Notificación de expiración Soporte para longitudes de clave de 2048 bit y cifrado SSL con 128 o 256 bit.
Certificado SSL Extended Validation (multidomain)	Asegura desde 2 (mínimo) hasta 250 dominios (con coste adicional por SAN adicional sobre el mínimo de 2) Asegura tanto el dominio www.dominio.com como dominio.com por defecto Algoritmos de hash: SHA-2 y ECC Número ilimitado de licencias de servidor Número ilimitado de reemisiones Validación extendida Tiempo de vida de hasta 825 días Notificación de expiración Soporte para longitudes de clave de 2048 bit y

	cifrado SSL con 128 o 256 bit.
Certificado SSL Wildcard	Asegura todos los subdominios del dominio *.dominio.com Asegura tanto los subdominios *.dominio.com como dominio.com Algoritmos de hash: SHA-2 y ECC Validación de organización Tiempo de vida de hasta 825 días Notificación de expiración Soporte para longitudes de clave de 2048 bit y cifrado SSL con 128 o 256 bit.
Certificado SSL Multidomain	Asegura desde 4 (mínimo) hasta 250 dominios (con coste adicional por SAN adicional sobre el mínimo de 4) Asegura tanto el dominio www.dominio.com como dominio.com por defecto Algoritmos de hash: SHA-2 y ECC Número ilimitado de licencias de servidor Número ilimitado de reemisiones Validación de organización Tiempo de vida de hasta 825 días Notificación de expiración Soporte para longitudes de clave de 2048 bit y cifrado SSL con 128 o 256 bit.

Para los tipos de certificado multidomain, tanto en versión EV como no, se ha de soportar de añadir dominios adicionales sobre el mínimo que contempla cada uno de ellos.

3.2. Características de la solución

Se detallan a continuación a modo de requisitos individuales las características que la solución debe obligatoriamente contemplar.

ID	Característica	Descripción
R1	Emisión de certificado SSL en versiones SSL, EV SSL y Multidominio	La plataforma al menos debe contemplar la emisión de este tipo de certificados, según se detallan en apartado previo.
R2	Compatibilidad con navegadores, teléfonos y dispositivos	Deben estar cubiertos como mínimo: 99,5% de navegadores de escritorio 94% de navegadores móviles 99,5% JRE
R3	Revocación y sustitución gratuita del certificado	Recuperación de certificados durante toda la vida del contrato, modelo pooling en el que se consume el derecho de uso (certificados reciclables).
R4	Certificados SSL: Emisión y revocación de certificados de forma inmediata	Emisión y revocacion on-line. Proceso previo de registro de dominios al inicio de contrato u on-line bajo demanda.
R5	Certificados SSL EV: Agilidad y flexibilidad en los tiempos de emisión.	Emisión y revocacion on-line. Proceso previo de registro según CA/Browser forum (www.cabforum.org)
R6	Herramienta única de administración.	Administración a través de herramienta online disponible 24x7.
R7	Administración centralizada de todos los certificados a través de la plataforma.	Gestión centralizada de todos los aspectos del ciclo de vida de los certificados (solicitud, emisión, renovación, revocación...)
R8	Acceso restringido a la consola de administración. Doble factor.	Login con usuario y contraseña añadiéndose un segundo factor de autenticación basado en tarjeta de coordenadas o Soft Token.
R9	Delegación de privilegios de	Es posible configurar clientes y sub-

	administración basado en entidades.	administradores para la gestión de certificados y dominios concretos.
R10	Informes en tiempo real.	Motor de informes en tiempo real que permita la generación de informes predefinidos y personalizados al menos por rangos de fechas, estado de certificados, dominios y clientes.
R11	Avisos y notificaciones.	Posibilidad de configurar avisos y notificaciones ante eventos de expiración y renovación de los certificados. Así mismo la notificación debe estar disponible para los contactos configurados durante los procesos de emisión.
R12	Registros de auditoria.	Capacidad para registrar todas las acciones sobre los certificados y todas las acciones de los administradores sobre la configuración de la herramienta.
R13	Flujos de trabajo para el seguimiento de las operaciones.	Aprobación de certificados con peticionarios y aprobadores. Notificaciones vía correo electrónico e interfaz web de la herramienta.
R14	Escaneo de páginas web básico para los certificados no EV.	Escaneo de malware con una escalabilidad de al menos 250 páginas y motor de búsqueda y monitorización de listas negras.
R15	Escaneo de páginas web avanzado para los certificados EV.	Escaneo de malware con una escalabilidad de al menos 500 páginas y motor de búsqueda y monitorización de listas negras, remedio de malware automático y escaneo de vulnerabilidades de páginas web.
R16	Dominios disponibles	Deben estar disponibles en la provisión inicial de la herramienta al menos 10 dominios.
R17	Organizaciones disponibles	Deben estar disponibles en la provisión inicial de la herramienta al menos 10 organizaciones.
R18	Cuentas de administrador disponibles	Deben estar disponibles en la provisión inicial de la herramienta al menos 10 cuentas de administración.

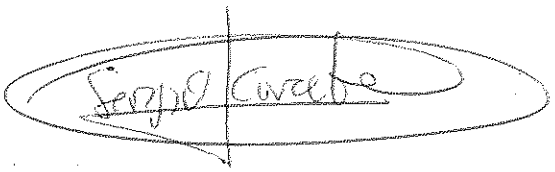
3.3. Servicio de soporte

En relación al servicio de soporte se han de contemplar los siguientes requisitos mínimos.

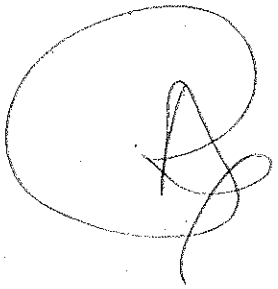
ID	Característica	Descripción
S1	Atención 8x5	Atención al menos en horario 8x5 en español e inglés.
S2	Consultas e incidencias	Servicio disponible tanto para consultas como para incidencias sobre la herramienta de gestión o certificados.
S3	Canales de atención	Disponibles tanto vía telefónica, como a través de portal de incidencias y email.
S4	Informes periódicos de atención a incidencias	Envío de informes periódicos para seguimiento y control del servicio.
S5	Contacto telefónico personalizado	Contacto telefónico personalizado sin menús ni colas telefónicas previas.
S6	Escalado ante emergencias	Atención con escalado ante emergencias disponible.

El soporte será cubierto en todo caso por la entidad de certificación que firma los certificados o por un partner reconocido y autorizado de la misma, siendo esta condición obligatoria objeto de cumplimiento.

22 de marzo de 2019



Firma: Sergio Cruceta Gómez
ÁREA INFRAESTRUCTURA INFORMÁTICA.



Firma: Ángel Rodríguez García
SUBDIRECCIÓN SISTEMAS INFORMATICOS

Firma: Pablo Galán González
DIRECCIÓN RECURSOS