

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN
DE UN SISTEMA DE GESTIÓN CENTRALIZADA DE CLAVES DE CERTIFICADOS EN
MODO SERVICIO Y EMISIÓN DE CERTIFICADOS ELECTRÓNICOS
EXPTE. GE. 09/2024**

1

Firmado Por	Jorge Miguel Soria Tonda	14/02/2024	Página 1/5
	Francisco Justo Serrano Lobato	14/02/2024	

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/2H9/xEa2rez059GdAF+E1w==>

Firmado Por	Alejandro Andujar Bors	29/02/2024	Página 1/5
-------------	-------------------------------	-------------------	------------

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/0DGLZVLRqbV+i3TC8tDaLQ==>

ÍNDICE

1. OBJETO DEL CONTRATO.	3
2. PRESCRIPCIONES TÉCNICAS.	3

Firmado Por	Jorge Miguel Soria Tonda	14/02/2024	Página 2/5
	Francisco Justo Serrano Lobato	14/02/2024	

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/2H9/xEa2rez059GdAF+E1w==>

Firmado Por	Alejandro Andujar Bors	29/02/2024	Página 2/5
-------------	------------------------	------------	------------

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/0DGLZVLRqbV+i3TC8tDaLQ==>

1. OBJETO DEL CONTRATO.

El objeto del presente pliego es fijar las condiciones que deben regir contratación de los siguientes servicios:

- Suministro de un sistema de gestión centralizada de claves en modo servicio
- Emisión de certificados electrónicos actuando LIPASAM como autoridad de registro.

2. PRESCRIPCIONES TÉCNICAS.

1. SOLUCIÓN DE CENTRALIZACIÓN DE CLAVES EN MODO SERVICIO, con mantenimiento de 2 años.

El sistema a implementar debe disponer al menos de los siguientes servicios:

- Gestión de operadores y administradores del sistema.
- Autoridad de Registro RA.
- Gestión centralizada del ciclo de vida de los certificados (renovaciones, revocaciones, control de caducidades, ...).
- Consulta pública de claves públicas de certificados.
- Políticas de certificación, documentación y formación.
- Emisión de certificados para diferentes usos:
 1. Firma.
 2. Cifrado.
 3. Autenticación.
 4. SmartCard Logon.
- Perfiles de emisión de certificados predefinidos:
 1. De empleado
 2. De apoderamiento especial
 3. De representante
 4. De persona jurídica
 5. De facturación electrónica
 6. De servidor
 7. Servidor de dominio
 8. De Sede electrónica
 9. De sello electrónico para la actuación automatizada.
- Almacenamiento centralizado en la nube en un entorno de alta seguridad que cumple con todos los estándares normativos vigentes (eIDAS-UE).

3

Firmado Por	Jorge Miguel Soria Tonda	14/02/2024	Página 3/5
	Francisco Justo Serrano Lobato	14/02/2024	

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/2H9/xEa2rez059GdAF+E1w==>

Firmado Por	Alejandro Andujar Bors	29/02/2024	Página 3/5
-------------	------------------------	------------	------------

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/0DGLZVLQbV+i3TC8tDaLQ==>

- Entorno de alta disponibilidad con duplicación de HSMs.
- Deben cumplir los estándares FIPS 140-2 Nivel 3 y Common Criteria EAL 4+.
- Posibilidad de definir políticas de uso de los certificados, tanto para acceso a sitios web como en aplicaciones.
- Posibilidad de establecer restricciones de acceso temporales (rango de fechas, días y horas).
- Posibilidad de delegar el uso de los certificados a terceros, pudiendo establecer políticas de uso y restricciones de acceso.
- Posibilidad de definir diferentes tipos de autenticación de usuario, incluyendo sistemas de autenticación robusta y de doble factor.
- Registro de la actividad y uso de los certificados.
- Disponibilidad del certificado desde múltiples entornos y dispositivos.
- Posibilidad de compatibilizar el uso de certificados locales y centralizados de forma que el usuario lo perciba como un repositorio único.
- La solución debe ser integrable con un servicio LDAP.
- Deben cumplir la legislación vigente.

2. CERTIFICADOS

El presente pliego contempla la emisión de los siguientes certificados electrónicos cualificados:

- 120 CERTIFICADOS DE PERTENENCIA A ENTIDAD, en modo servicio, con una validez de 2 años
- 10 CERTIFICADOS DE PERTENENCIA A ENTIDAD, claves almacenadas en software, y gestionadas en modo servicio, con una validez de 2 años
- 5 CERTIFICADOS DE REPRESENTANTE ANTE LAS ADMINISTRACIONES PÚBLICAS, en modo servicio, con una validez de 2 años
- 1 CERTIFICADO DE SELLO ELECTRONICO, algoritmo de firma SHA256, longitud de clave 2048 bits RSA, con validez de 2 años
- 1 CERTIFICADO DE SERVIDOR SSL OV MULTIDOMINIO SHA256 con una validez de 2 años que satisfaga:
 - Por un lado, certificar que un determinado dominio ha sido registrado a nombre de la entidad identificada en el certificado. (No cabe la posibilidad de suplantaciones de identidad).
 - Por otro lado, debido al empleo del protocolo SSL, garantizar que la comunicación entre el cliente y el servidor es totalmente confidencial y que no podrá ser interceptada ni modificada por un tercero.

4

Firmado Por	Jorge Miguel Soria Tonda	14/02/2024	Página 4/5
	Francisco Justo Serrano Lobato	14/02/2024	

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/2H9/xEa2rez059GdAF+Elw==>

Firmado Por	Alejandro Andujar Bors	29/02/2024	Página 4/5
-------------	-------------------------------	-------------------	------------

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/0DGLZVLQqbV+i3TC8tDaLQ==>

- iii. Los certificados elegidos deben ser reconocidos por todos los navegadores de internet más reconocidos (Internet Explorer, Chrome, Firefox) sin la realización de trabajos adicionales.

Los certificados deben cumplir

- Certificados electrónicos cualificados de nivel alto.
- Los certificados deben cumplir con los estándares x.509v3 y ser certificados cualificados conforme al Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Además:
 - Certificados válidos para uso interno o externo.
 - Certificados personales, ya que el certificado se emite con los datos del firmante.
 - Permitir firma digital de elementos de escritorio.
 - Firma digital de documentos Office y Adobe Acrobat.
 - Autenticación de cliente y control de acceso a aplicaciones.
 - Firma de formularios.
 - Estar reconocidos por los navegadores de internet más habituales como Chrome, Firefox y Microsoft Edge, sin la realización de trabajos adicionales.

Tiempo máximo de implantación: 22 días hábiles.

La validez máxima de los certificados emitidos deberá ser de 24 meses, y su renovación deberá contemplarse 30 días antes de la fecha de caducidad de los mismos.

Firmado Por	Jorge Miguel Soria Tonda	14/02/2024	Página 5/5
	Francisco Justo Serrano Lobato	14/02/2024	

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/2H9/xEa2rez059GdAF+E1w==>

Firmado Por	Alejandro Andujar Bors	29/02/2024	Página 5/5
-------------	------------------------	------------	------------

Este documento tiene carácter de copia auténtica (Ley 39/2015, de 1 de Octubre y Decreto 60/2018, de 12 de Julio).Verifique su integridad en:

<https://portafirmas.lipasam.es:8443/verifirma/code/0DGLZVLRqbV+i3TC8tDaLQ==>