Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

POLÍTICA Y PRÁCTICAS DEL SERVICIO DE FIRMA EN SERVIDOR

	NOMBRE	FECHA
Elaborado por:	FNMT-RCM	12/12/2019
Revisado por:	FNMT-RCM	06/02/2020
Aprobado por:	FNMT-RCM	03/03/2020

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	12/12/2019	Creación del documento	FNMT-RCM

Referencia: DPSCST/SSASP PS/SGPSC/2019

Documento clasificado como: *Público*

ÍNDICE DE CONTENIDOS

1. REFERENCIAS

[DGPC] - Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica (http://www.cert.fnmt.es/dpcs/)

[ETSI EN 319 401] - General Policy Requirements for Trust Service Providers

[ETSI EN 319 411-1] - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSI TS 119 431-1] - TSP service components operating a remote QSCD / SCDev

[CEN EN 419 241-1]: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

2. ACRÓNIMOS Y DEFINICIONES

1. A las definiciones dispuestas en la DGPC, para la interpretación del presente documento se añaden los siguientes términos y abreviaturas tal y como se definen en ETSI TS 119 431-1:

- *autenticación:* un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico
- *identificación electrónica (eID):* el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.
- *medios de identificación electrónica:* una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.
- *referencia a medios de identificación electrónica:* datos usados en el SSASC como referencia a unos medios de identificación electrónica que permiten autenticar a un firmante.
- *dispositivo cualificado de creación de firma / sello electrónico (QSCD):* dispositivo de creación de firma que cumple con los requisitos del Anexos II del Reglamento(EU) No 910/2014.
- *dispositivo remoto de creación de firma:* dispositivo de creación de firma utilizado a distancia por el firmante y operado en su nombre bajo su control exclusivo de uso.
- *componente de servicio de aplicación de firma en servidor (SSASC):* componente de servicio operado por un TSP, compuesto de una aplicación de firma en servidor (SSA) y un QSCD / SCdev, empleado para la creación de firmas electrónicas en nombre del firmante.
- *proveedor de servicio de aplicación de firma en servidor (SSASP):* TSP que opera un SSASC.
- *dispositivo de creación de firma (SCDev o SCD):* un equipo o programa informático configurado que se utiliza para crear una firma electrónica.

(Los términos señalados en cursiva se definen en el presente documento o en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica)

3. INTRODUCCIÓN Y OBJETO

2. La Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, de aquí en adelante FNMT-RCM, es un Prestador cualificado de Servicios de Confianza de conformidad con el Reglamento (UE) No 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 y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

3. Este documento contiene la *Política y Declaración Prácticas del servicio de firma en servidor* de la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda.

4. El servicio de firma en servidor es un servicio en que Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda gestiona en nombre del firmante su dispositivo de creación de firma permitiéndole generar firma electrónica a distancia asegurando el control exclusivo sobre sus claves de firma.

5. El presente documento se estructura de acuerdo a la especificación técnica ETSI TS 119 431

4. ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento define la *Política y Prácticas del Servicio de Firma en Servidor*, forma parte integrante de la *Declaración General de Prácticas de Certificación* (DGPC) de la FNMT-RCM, como *Prestador de Servicios de Confianza* (PSC).

7. Este es un documento declarativo en el que se describen los aspectos más relevantes del *Servicio de firma en servidor* y la operativa de los componentes que gestionan dispositivos de creación de firma a distancia en nombre del firmante. Asimismo, se proporciona una autodeclaración de las medidas de salvaguarda de la infraestructura y de los controles de seguridad técnicos y no técnicos aplicados a los sistemas participantes en la prestación del servicio.

8. Los componentes del servicio consisten en la aplicación de creación de firma y el dispositivo de creación de firma que podrá tener el carácter de cualificado de acuerdo con la definición del Anexo II del Reglamento (UE) 910/2014.

9. La presente Política y Declaración de Prácticas es aplicable a las claves de todos los certificados de firma electrónica emitidos por la FNMT-RCM que se definan en su Declaración de Prácticas de Certificación como certificados de firma electrónica centralizada.

10. Como quiera que la prestación del *Servicio de firma en servidor* se enmarca dentro de los Servicios de Confianza de la FNMT-RCM, es de aplicación lo referido en la [DGPC] sobre el régimen de responsabilidad aplicable a los miembros de la *Comunidad Electrónica* y terceros que confían en dichos servicios, los controles de seguridad aplicados a sus procedimientos e instalaciones, la protección de datos de carácter personal y demás cuestiones de tipo informativo relacionadas con el citado servicio.

4.1. RELACIÓN ENTRE EL PRESTADOR Y EL SERVICIO DE FIRMA EN SERVIDOR

11. El *componente de servicio de aplicación de firma en servidor (SSASC)* forma parte de los servicios operados por FNMT-RCM y permite prestar el servicio de firma electrónica a distancia a los firmantes que cuentan con un certificado electrónico definido para firma centralizada en su correspondiente Declaración de Prácticas de Certificación.

12. En el presente documento la FNMT-RCM es identificada como el SSASP

13. En calidad de SSASP, la FNMT-RCM desarrolla, implementa, hace cumplir y actualiza el presente documento que contiene la Política y la Declaración de Practicas de SSASC.

5. DISPOSICIONES GENERALES DE LA POLÍTICA Y DE LA DECLARACIÓN DE PRÁCTICAS

5.1. REQUISITOS GENERALES DE LA DECLARACIÓN DE PRÁCTICAS

14. La FNMT-RCM en la prestación de su servicio de firma en servidor emplea dispositivos criptográficos de creación y protección de firmas catalogados como cualificados (QSCD) de conformidad con el Reglamento (UE) No 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 y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

15. Los HSM son operados de acuerdo con su certificación FIPS 140-2 level 3 y la solución SSASC empleada está alineada con los requisitos de seguridad definidos en la norma EN 419 241-1 para poder actuar como un Trustworthy System Supporting Server Signing (TW4S) con Sole Control Level 2 (SCAL2).

5.1.1. Administración del documento.

16. Véase apartado 1.5 de la DGPC

5.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

17. La presente *Política del Servicio de firma en servidor* tiene la siguiente identificación:

Nombre	*Política del Servicio de firma en servidor* de la FNMT-RCM
Referencia/OID	0.4.0.19431.1.1.3 - EUSCP: EU SSASC Policy
Versión	1.0
Localización	http://www.cert.fnmt.es/dpcs/
DPC relacionada	Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica de la FNMT-RCM.

	Políticas y prácticas de certificación de certificados de firma electrónica y sello electrónico del Sector Público Políticas y prácticas de certificación particulares en el ámbito de las Administraciones Públicas, organismos y entidades de derecho público
Localización	http://www.cert.fnmt.es/dpcs/

18. El *Servicio de firma en servidor* que provee la FNMT-RCM, como *Prestador cualificado de Servicios de Confianza*, se presta de conformidad con los requisitos del Reglamento eIDAS y el estándar europeo ETSI TS 119 431: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remoteQSCD / SCDev.

19. La FNMT-RCM revisa periódicamente la conformidad de sus políticas con respecto a la especificación ETSI TS 119 431-1 y cambiará el identificador de sus políticas ante cualquier cambio en las políticas definidas en la sección 4.3.2 de dicha especificación.

5.3. PARTES INTERVINIENTES

20. Las partes que intervienen en la gestión y uso de los Servicios de Confianza descritos en la presente DGPC son las siguientes:

    1. Proveedor del servicio de firma remota (SSASP)
    2. Suscriptores y firmantes de los Certificados
    3. Partes que confían

5.3.1. Proveedor del servicio de firma remota (SSASP).

21. La FNMT-RCM actúa como *proveedor de servicio de aplicación de firma en servidor (SSASP)* y no delega ninguna parte del servicio a entidades terceras.

5.3.2. Suscriptores y firmante de los certificados.

22. El *Suscriptor* de un Certificado puede ser una entidad diferente de la figura de *Firmante* cuando hay una relación de representación o pertenencia a una Organización, de forma que ésta última es considerada la entidad Suscriptora, o cuando se trate de Certificados de Sello electrónico. No obstante, cada Declaración de Políticas de Certificación Particulares determinará esta posible separación entre las figuras del *Firmante* y el *Suscriptor*.

23. Los *Firmantes* son las personas físicas que mantienen bajo su uso exclusivo los Datos de creación de firma asociados a los *Certificados* de los que son *Titulares*.

5.3.3. Partes que confían.

24. Las partes que confían son aquellas personas físicas o jurídicas, diferentes del *Firmante* / *Suscriptor*, que reciben y / o usan *Certificados* y / o firmas electrónicas expedidos por la

FNMT-RCM y, como tales, les es de aplicación lo establecido por la correspondiente DPC cuando deciden confiar efectivamente en tales *Certificados*.

6. PRÁCTICAS DEL PROVEEDOR DE SERVICIOS DE CONFIANZA

6.1. RESPONSABILIDADES DE PUBLICACIÓN Y DEPÓSITO

25. Véase apartado 2 de la DGPC.

6.2. INICIALIZACIÓN DE LAS CLAVES DE FIRMA

6.2.1. Generación de claves de firma

26. Las operaciones de inicialización y administración del módulo criptográfico requieren de control dual.

27. Tras el proceso de registro de los usuarios, el correspondiente par de claves es generado dentro del HSM, certificado con FIPS PUB 140-2 L3, para realizar todas las operaciones criptográficas con las claves de los firmantes. Las claves de los firmantes son claves RSA con una longitud de clave de 2048 bits.

28. Junto a las claves del firmante, se genera una petición de certificado en formato PKCS #10 que sirve como prueba de posesión de la clave privada del firmante en el proceso de registro del certificado y emisión del certificado por parte de la Autoridad de Certificación.

29. Las *Claves privadas* asociadas a los *Certificados de Firma Centralizada para Empleado Público* son generadas y custodiadas por el módulo de activación de firma de la FNMT-RCM, de forma que el acceso a dichas *Claves* se realiza por medios que garantizan el control exclusivo por parte del *Firmante*.

30. Las claves se encontrarán en estado no activo y no se permitirá su uso hasta que no se haya completado el proceso de vinculación con la identidad del firmante a través de la emisión del certificado.

6.2.2. Asociación de los medios de identificación electrónica del firmante

31. La FNMT-RCM no delega el proceso de identificación y autenticación del firmante a terceras partes.

32. La Autoridad de Registro validará la identidad del firmante de acuerdo con los requisitos establecidos en la Declaración de Prácticas de Certificación Particulares del certificado, recabando la aceptación de los términos y condiciones de uso relativos al servicio y los medios de identificación electrónica.

33. Completado el proceso de identificación, la Autoridad de Registro de la FNMT-RCM entregará al firmante unas credenciales de identidad que le permitirán autenticarse en el *Portal de Gestión de Identidades* con un nivel de aseguramiento alto e iniciar el proceso de creación de su identidad de firma. En este proceso se requiere que el firmante cambie la contraseña de sus credenciales de identidad inicialmente otorgada por la Autoridad de Registro, y establezca la contraseña de activación de firma.

34. El SSASC protegerá la integridad de las credenciales de identificación mediante el cómputo de una función hash SHA1 con SALT.

6.2.3. Asociación del certificado del firmante

35. La identidad de firma se compone de un par de claves RSA con longitud 2048 y el certificado electrónico que vincula la clave pública a la identidad del firmante.

36. Hasta la efectiva asociación del certificado con su correspondiente par de claves, la identidad de firma es incompleta y el SSASC no permitirá el uso de las claves.

37. El SSASC solicitará al dispositivo QSCD la generación del par de claves de los firmantes antes de la emisión del certificado electrónico. Como requisito previo a la generación de las claves, el firmante deberá establecer el PIN/contraseña de activación de firma.

38. Así mismo, el SSASC solicitará a la correspondiente Autoridad de Certificación la emisión del certificado, el cual se pondrá a disposición del firmante a través del Portal de Gestión de Identidades.

39. El SSASC verifica que el certificado del firmante y la clave pública almacenada en el sistema se corresponden. En caso de que ambas claves públicas coincidan, el certificado queda vinculado al par de claves del firmante, completando la identidad de firma. La clave del firmante queda a partir de este momento operativa para realizar operaciones de firma.

40. La integridad de cada identidad de firma, se garantiza mediante la firma electrónica de cada registro en el repositorio donde se almacenan.

6.3. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LAS CLAVES DE FIRMA

6.3.1. Activación de las claves de firma

41. El módulo SAM dentro del entorno protegido aplicará el control de acceso del usuario sobre sus claves de firma. Esto se materializará por medio de un protocolo de activación de la firma (SAP, Signature Activation Protocol) con el que se generará unos datos de activación de firma (SAD, Signature Activation Data) sobre los que el SAM aplicará las condiciones de acceso al material de firma en el QSCD.

42. Las claves del firmante solo se pueden activar dentro del módulo HSM. La clave de un firmante sólo se podrá activar si completa el protocolo de activación autenticándose con sus credenciales de identidad y un OTP enviado a la cuenta de correo asociada a sus credenciales o bien autenticándose con un certificado cualificado. En ambos casos, la activación de las claves de firma requerirá el PIN/contraseña de firma, establecido previamente por el firmante.

43. El protocolo de activación de firma (SAP) está diseñado para prevenir ataques de man-in-themiddle y replay. Además de esto el mensaje SAD incorpora protecciones contra suplantación, robo de sesión, duplicación, robo de credenciales, phishing y adivinación, mediante la combinación de técnicas de cifrado, firma electrónica, funciones resumen, incorporación de números aleatorios y uso de dos factores de autenticación de diferente naturaleza. Todas las comunicaciones con el SSASC son protegidas mediante el protocolo TLS 1.2.

44. Los controles de acceso implementados en el SSA garantizan que un firmante no tiene acceso las claves de otros firmantes ni a otros objetos y funciones del sistema que no sean las funciones de firma.

45. Una vez se activa la clave del firmante el SSASC solo permite un único uso para firmar el resumen criptográfico contenido en el mensaje SAD utilizado para la activación. Tras la realización de la operación de firma solicitada, se requerirá un nuevo SAD para generar una nueva firma.

46. Las claves de los firmantes se almacenan cifradas en la base de datos del SSA utilizando el algoritmo de cifrado AES y una longitud de clave de 256 bits. La clave de cifrado para cada clave y firmante es diferente y se deriva a partir de una clave maestra del módulo criptográfico y el PIN/contraseña de activación de clave que establece el firmante.

47. El SSA permite generar firmas electrónicas con el algoritmo RSA PKCS#1 v1.5 y algoritmo resumen SHA-256.

6.3.2. Borrado de las claves de firma

48. Las claves del firmante son borradas de forma inmediata de la base de datos del SSA, cuando el certificado del firmante es revocado.

49. Periódicamente FNMT-RCM ejecuta un proceso de borrado de la base de datos del SSA, de aquellas claves de los firmantes cuyo certificado asociado ha caducado.

50. Los firmantes podrán solicitar la revocación de su certificado electrónico siguiendo los mecanismos establecidos en la Declaración de Prácticas de Certificación correspondiente. La revocación y caducidad del certificado supone en todos los casos la destrucción las claves asociadas.

6.3.3. Copia de seguridad y restauración de las claves de firma

51. Se mantienen copias de seguridad periódicas de la base de datos del SSA, donde se encuentra las claves de los firmantes, y del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente. El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio.

52. Las claves de infraestructura del SSASC son siempre almacenadas en contenedores cifrados.

53. El módulo criptográfico que contiene la clave maestra del SSASC que protege las claves de todos los firmantes requiere de control dual para su operación, copia de seguridad y restauración. La clave maestra del SSASC nunca abandona el módulo criptográfico en claro.

6.4. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTO Y DE PERSONAL

6.4.1. Generales

54. Véase apartado 5 de la DGPC

6.4.2. Controles de seguridad física

55. Véase apartado 5.1 de la DGPC

6.4.3. Controles de procedimientos

56. Véase apartado 5.2 de la DGPC

6.4.4. Controles de personal

57. Véase apartado 5.3 de la DGPC

6.4.5. Procedimientos de auditoría de seguridad

58. Véase apartado 5.4 de la DGPC. Además, en particular, en la prestación del servicio de firma electrónica en servidor:

59. El SSA guarda registro, al menos, de los siguientes eventos:

- Inicialización de sistema, arranque, parada y cambios de configuración.
- Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción)
- Uso de claves de los firmantes.
- Autenticación de los firmantes (incluyendo intentos fallidos).
- Gestión de los datos de activación de firma del firmante (cambios de PIN/contraseña)
- Accesos al sistema por parte de los usuarios administradores.

60. El SSA genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores.

61. El SSA protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando una función HMAC que encadena cada registro con el anterior.

62. Todos los registros de eventos del registro de auditoría del SSA incluyen la siguiente información:

- Fecha y hora del evento.
- Tipo de evento.
- Identidad de la entidad (firmante, administrador o proceso) responsable de la acción.
- Resultado del evento (éxito o error)

63. El SSA comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSA dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema.

64. Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP utilizando como referencia el ROA (Real Observatorio de la Armada). Existen controles para detectar problemas que puedan comprometer la sincronización.

6.4.6. Archivo de registros

65. Véase apartado 5.5 de la DGPC

6.4.7. Cambio de claves de la CA

66. Véase apartado 5.6 de la DGPC

6.4.8. Compromiso de claves y recuperación de desastre

67. Véase apartado 5.7 de la DGPC

6.4.9. Cese de la actividad

68. Véase apartado 5.8 de la DGPC

6.5. CONTROLES DE SEGURIDAD TÉCNICA

6.5.1. Gestión de los sistemas de la seguridad

69. El SSA implementa los siguientes roles de gestión:

- Responsable de seguridad (security officer): tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.
- Administrador del sistema (system administrators): es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.
- Operador del sistema (system operators): es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.
- Auditor del sistema (system auditor): está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

70. FNMT-RCM asigna estos roles a personal cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1.

6.5.2. Operaciones y Sistemas

71. La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC.

72. El componte software SSA y el módulo HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos su certificación como dispositivo QSCD.

6.5.3. Controles de seguridad informática

73. Véase apartado 6.5 de la DGPC

74. El SSASC se encuentra monitorizado y se generan alertas que son enviadas a los administradores del sistema cuando se detectan eventos que pueden impactar en su disponibilidad o comprometer su seguridad.

6.5.4. Controles técnicos del ciclo de vida

75. Véase apartado 6.6 de la DGPC y los correspondientes en cada una de las Políticas y Prácticas Particulares

6.5.5. Controles de seguridad de red

76. Véase apartado 6.7 de la DGPC

6.6. AUDITORÍA DE CONFORMIDAD

77. En este apartado será de aplicación general lo descrito en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica, y adicionalmente lo especificado en el presente apartado.

78. El Servicio de firma en servidor ofrecido por la FNMT-RCM está sujeto a auditorías periódicas, según el esquema de certificación correspondiente a los Prestadores de Servicios de Confianza, en cuanto al cumplimiento de los requisitos definidos por los estándares europeos ETSI EN 319 401 "General Policy Requirements for Trust Service Providers", ETSI TS 119 431-1 – "TSP service components operating a remote QSCD / SCDev".

79. Las auditorías mencionadas en el apartado anterior son realizadas anualmente por un organismo acreditado para tal fin.

6.7. OTROS ASUNTOS LEGALES Y DE ACTIVIDAD

6.7.1. Tarifas

80. FNMT-RCM aplicará a las Administraciones Públicas las tarifas aprobadas por la Subsecretaría de la cual depende para la prestación de los servicios de confianza o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizado para tal efecto.

81. Las tarifas a aplicar al sector privado se rigen por el contrato suscrito para la provisión del Servicio de firma en servidor. Adicionalmente, la FNMT – RCM podrá establecer las tarifas y los medios de pago que considere oportunos en cada momento. El precio y condiciones de pago podrán ser consultados en la página web de la FNMT – RCM o bien serán facilitados por el área comercial correspondiente bajo petición a la dirección de correo electrónico comercial.ceres@fnmt.es.

82. Los requisitos de política definidos en el presente documento no implican ninguna restricción en el cobro del Servicio de firma en servidor.

6.7.2. Responsabilidad financiera

83. Véase apartado 9.2 de la DGPC

6.7.3. Confidencialidad dela información

84. Véase apartado 9.3 de la DGPC

6.7.4. Protección de datos personales

85. Véase apartado 9.4 de la DGPC

6.7.5. Derechos de propiedad intelectual

86. Véase apartado 9.5 de la DGPC

6.7.6. Obligaciones y garantías

87. Véase apartado 9.6 de la DGPC

6.7.7. Rechazo de otras garantías

88. Véase apartado 9.7 de la DGPC

6.7.8. Limitación de responsabilidades

89. Véase apartado 9.8 de la DGPC

6.7.9. Indemnizaciones

90. Véase apartado 9.9 de la DGPC

6.7.10. Caso fortuito y fuerza mayor

91. Véase apartado 9.16 de la DGPC

6.7.11. Notificaciones individuales y comunicación con los participantes

92. Véase apartado 9.11 de la DGPC

6.7.12. Modificaciones de este documento

93. Véase apartado 9.12 de la DGPC

6.7.13. Reclamaciones y resolución de disputas

94. Véase apartado 9.13 de la DGPC

6.7.14. Normativa de aplicación

95. Además de lo indicado en el apartado 9.14 de la DGPC, será de aplicación los siguientes estádares:

ETSI TS 119 431: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

6.7.15. Cláusula de jurisdicción competente

96. Véase apartado 9.14 de la DGPC

6.7.16. Otras provisiones

97. Véase apartado 9.17 de la DGPC