SECRETARÍA DE ESTADO DE DEFENSA

DIRECCIÓN GENERAL DE INFRAESTRUCTURA

SUBDIRECCIÓN GENERAL TIC

PO-345-SEGINFO/02/14/V1

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC) DE LA WAN DE PROPÓSITO GENERAL DEL MINISTERIO DE DEFENSA.

O.I.D: (2) (16) (724) (1) (1) (1) (1) (3) (0) (1)

CONTROL DE DOCUMENTACIÓN	
COPIA CONTROLADA Nº	COPIA 1
FECHA DE LA COPIA	02 / 09 / 2014
COPIA ASIGNADA A:	DISTRIBUCIÓN
FIRMA AUTORIZADA DE REGISTRO	DURA GONZALEZ JAVIER | 00812999H, Capitán Firmado digitalmente por DURA GONZALEZ JAVIER | 00812999H, Capitán Nombre de reconocimiento (DN): c=ES, o=MDEF, ou=PERSONAS, ou=certificado electrónico de empleado público, serialNumber=00812999H, cn=DURA GONZALEZ JAVIER | 00812999H Motivo: Registro Fecha: 2014.09.04 09:16:09 +02'00'

SEPTIEMBRE /2014

DOCUMENTO

Título:	Declaración de Prácticas de Certificación del Ministerio de Defensa.				
Categoría:	*Identidad Digital*	Versión del Documento:	*1.8*	Fecha:	*01/09/2014*
Departamento:	*Subdirección General de Tecnologías de la Información y Comunicaciones*				
Área:	*Área de Seguridad de la Información*				

CONTROL DE FIRMAS

RESPONSABLE DEL SERVICIO	RESPONSABLE DE SEGURIDAD	RESPONSABLE DE LA INFORMACIÓN
Jefe de la Unidad de Apoyo y Coordinación del Área de Seguridad de la Información	**Jefe del Área de Seguridad de la Información de la SDGTIC**	**Subdirector General de Tecnologías de la Información y Comunicaciones y AGPMD**
DELGADO DE LUQUE JOSE GONZALO | 28683636Z Firmado digitalmente por DELGADO DE LUQUE JOSE GONZALO |28683636Z Nombre de reconocimiento (DN): c=ES, o=MDEF, ou=PERSONAS, ou=certificado electrónico de empleado público, serialNumber=28683636Z, cn=DELGADO DE LUQUE JOSE GONZALO |28683636Z Fecha: 2014.09.01 12:40:12 +02'00'	PEREZ SANCHEZ MIGUEL ANGEL |21632971E Firmado digitalmente por PEREZ SANCHEZ MIGUEL ANGEL | 21632971E Nombre de reconocimiento (DN): c=ES, o=MDEF, ou=PERSONAS, cn=PEREZ SANCHEZ MIGUEL ANGEL |21632971E Fecha: 2014.09.02 09:50:40 +02'00'	GOBERNA CARIDE JOSE LUIS |36020616V, Subdirector General de Tecnologías de Información y Comunicaciones Firmado digitalmente por GOBERNA CARIDE JOSE LUIS |36020616V, Subdirector General de Tecnologías de Información y Comunicaciones Nombre de reconocimiento (DN): c=ES, o=MDEF, ou=PERSONAS, ou=certificado electrónico de empleado público, serialNumber=36020616V, cn=GOBERNA CARIDE JOSE LUIS |36020616V Fecha: 2014.09.02 11:25:09 +02'00'

CONTROL DE CAMBIOS

VERSIÓN	REVISIÓN	FECHA	OBSERVACIONES
1	0	19/09/2006	Versión inicial.
1	1	15/04/2008	Cambios menores.
1	2	16/02/2009	Actualización siguiendo los comentarios del Informe Preliminar del MITyC, para adaptar la Declaración de Prácticas de Certificación a lo exigido por la Ley 59/2003 y poder ser reconocido el Ministerio de Defensa como PSC.
1	3	20/07/2009	Cambio en el OID descriptivo de la CPS para evitar confusiones de nomenclatura. Añadido MINISDEF como PSC y firma electrónica reconocida. Cambios en los perfiles de certificados: • Quitada la criticidad de la extensión CertificatePolicies. Modificados OIDs extensión CertificatePolicies. Añadidos CRLDistributionPoint en HTTP. Extensión SubjectAltName en los certificados de las ECs. Extensión IssuerAltName en el certificado de firma reconocida de persona. • Cambiados perfiles de los componentes de la PKI

			tras la recertificación 13/7/2009
1	4	01/12/2010	Adaptación DPC a RFC 3647 Indicación de que la DPC se ajusta a lo establecido en los artículos 18,19 y 20 del Real Decreto 4/2010. Añadidos nuevos perfiles de certificados derivados Ley 11/2007. Modificados perfiles anteriores para armonizar extensiones con los nuevos. Añadidos OIDs de los perfiles de certificados Claves 2048 bits para todos los certificados en TEMD Tratamiento extensión “Policy Constraints”: No estipulado Añadidos descripción de los perfiles de los certificados en detalle en el Anexo2
1	5	31/10/2011	Modificación domicilio PKIDEF por Arturo Soria 289, 28071 Madrid Cambio status TEMD v1.0 Sustitución RETEMSA por LUNA CA
1	6	31/01/2012	Revisión de las certificaciones NIST y CC de los HSM
1	7	15/02/2013	Eliminada la extensión "Qualified Certificate Statements" en los certificados de Sede, siguiendo la Política de Firma Electrónica y de Certificados de la AGE. Modificado el Perfil de CRL y ARL para adecuarse al estándar ya que las incompatibilidades con productos Microsoft se han solventado.
1	8	01/09/2014	Revisión. Eliminación HSM retirados de servicio. Cambio de “Departamento PKIDEF” por “Subunidad de PKI”.

ÍNDICE

ÍNDICE DE FIGURAS Y TABLAS

1 INTRODUCCIÓN

1.1 *Visión General*

El Ministerio de Defensa, mediante la Orden DEF/315/2002, de 14 de Febrero, aprobó el Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa que definía la necesidad de implantar una Infraestructura de Clave Pública en la Red de Propósito General (en adelante **PKIDEF**) para emitir y gestionar de forma adecuada certificados digitales que proporcionasen servicios de seguridad como autenticación de usuarios, no repudio de las comunicaciones y confidencialidad. Adicionalmente, se determinó el diseño y fabricación de un dispositivo de alta seguridad (con requisitos de seguridad equivalentes a una certificación CC EAL4+), la Tarjeta Electrónica del Ministerio de Defensa (**TEMD**), que permitiese la utilización de certificados electrónicos y el manejo de claves en entornos de alta seguridad.

Con fecha de 29 de abril de 2009 el Ministerio de Industria, Turismo y Comercio dicta la resolución por la que, de acuerdo con lo dispuesto en la ley 59/2003 de firma electrónica, se inscribe al Ministerio de Defensa en el registro de prestadores de servicios de certificación que expide certificados reconocidos de firma. En consecuencia, y de acuerdo con lo previsto en esa misma ley, la firma electrónica creada con la tarjeta electrónica del Ministerio de Defensa, cuyo uso está regulado en la Orden Ministerial 3/2008, tiene el carácter de firma electrónica avanzada (basada en un certificado reconocido). De esta forma se dota a la totalidad de los usuarios del Ministerio de Defensa de un servicio global de Identidad Digital basado en certificados electrónicos, que permite la autenticación fuerte frente a los sistemas de información, el tratamiento de la información electrónica de forma íntegra y segura, además de permitir la firma de documentos de forma electrónica.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos consagra el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos, estableciendo los sistemas de firma electrónica que pueden utilizarse para identificación electrónica de las administraciones (SEDE ELECTRÓNICA), para la actuación administrativa automatizada (SELLO ELECTRÓNICO) y para la firma electrónica del personal al servicio de las Administraciones Públicas (EMPLEADO PÚBLICO).

Tras la aprobación de las diferentes referencias normativas que han seguido a la Ley 11/2007 (Reglamento de desarrollo de la Ley 11/2007, Esquema Nacional de Seguridad y Esquema Nacional de Interoperabilidad), en donde se han establecido los perfiles comunes de los certificados digitales para que puedan interoperar en todas las Administraciones Públicas, el Ministerio de Defensa ha elaborado y definido unos perfiles propios de Sede Electrónica, Sello Electrónico y Empleado Público para ser emitidos por PKIDEF. Así, los certificados que se emiten bajo estos perfiles tienen la estructura propuesta en el esquema de identificación y firma de las Administraciones Públicas para facilitar las operaciones de interoperabilidad y de aceptación en la Administración General del Estado y en las restantes Administraciones Públicas.

Por otro lado, el Ministerio de Defensa posee una Entidad de Sellado de Tiempo que, cumpliendo los estándares internacionales (RFC 3161, ETSI TS 102 023), está sincronizada con los servidores de tiempo NTP del Real Instituto y Observatorio de la Armada en España (que determina la hora oficial en España) proporcionando plenas garantías legales y económicas para dar servicios relacionados con firma electrónica y el sellado de tiempo.

De acuerdo con lo anterior y en cumplimiento de la previsión legal contenida en el artículo 19 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, la presente Declaración de Prácticas de Certificación (**DPC**) detalla las normas y condiciones generales de los servicios de certificación que presta el Ministerio de Defensa, en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso, la existencia de procedimientos de coordinación con los registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

De esta forma, la presente DPC recoge las normas aplicables a la actividad del Ministerio de Defensa como Prestador de Servicios de Certificación para la Red de Propósito General, describiendo tanto los procedimientos como los mecanismos técnicos que garantizan los niveles de seguridad exigidos en la Política de Certificación del Ministerio de Defensa:

- *La presente DPC rige el comportamiento y operativa de los certificados de nivel de confianza de clase 2 en soporte hardware y software, tal y como se identifican en la Política de Certificación del Ministerio de Defensa.*
- *La Autoridad de Gestión de PKI del Ministerio de Defensa (AGPMD), autoriza la implantación y operación a través de la Subunidad de PKI, dependiente de la Unidad de Apoyo y servicios Comunes del CCEA, de una Infraestructura de Clave Pública (**PKIDEF**) que dote a los usuarios de la Red de Propósito General del Ministerio de Defensa de los certificados digitales necesarios.*

La presente DPC se ha estructurado conforme a lo dispuesto por el grupo de trabajo PKIX del IETF (Internet Engineering Task Force), en su documento de referencia RFC 3647 (aprobado en Noviembre de 2003) “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC 3647. Cuando no se haya previsto nada en alguna sección aparecerá la frase “No estipulado”.

Este documento está sujeto a la legislación española. Explícitamente se asumen como de aplicación obligatoria las siguientes normas:

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- La Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

- La directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Ley Orgánica 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal.

En concreto, el presente documento se ajusta a lo establecido en los artículos 18,19 y 20 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Los perfiles de los certificados indicados en el presente documento y emitidos por la PKI del Ministerio de Defensa se ajustan a la "Política de firma electrónica y de certificados de la Administración General del Estado", garantizando que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa.
- De acuerdo con lo previsto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, sobre obligaciones de los prestadores de servicios de certificación, el Ministerio de Defensa recoge en esta Declaración de Prácticas de Certificación todos los aspectos demandados en relación con la interoperabilidad organizativa, la interoperabilidad semántica y la interoperabilidad técnica.
- El Ministerio de Defensa proporcionará la información necesaria a aquellas Plataformas de validación de certificados electrónicos y de firma electrónica que sigan lo indicado en el Real Decreto 4/2010. De esta forma se permite acceder de forma alternativa, a aquellas aplicaciones de diversos ámbitos de las Administraciones públicas que sean consumidoras de los servicios de certificación ofrecidos por el Ministerio de Defensa, a todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios.

De igual manera, la DPC recoge la Normativa Interna del Ministerio de Defensa, en los términos de responsabilidades y obligaciones de uso al personal en posesión de certificados digitales y la TEMD:

- Orden Ministerial 3/2008, de 8 de enero, por la que se aprueba la Normativa que regula la Tarjeta Electrónica del Ministerio de Defensa.
- Instrucción 4/2009, de 23 de enero, del Secretario de Estado de Defensa, por la que se aprueba la Normativa que regula los procedimientos de uso de la Tarjeta Electrónica del Ministerio de Defensa.
  - Instrucción 75/2013, de 22 de noviembre, del Secretario de Estado de Defensa, por la que se modifica la Instrucción 4/2009, de 23 de enero, del Secretario de Estado de Defensa que aprueba la normativa que regula los procedimientos de uso de la Tarjeta Electrónica del Ministerio de Defensa.

Es obligado el conocimiento de la presente DPC entre los subscriptores y usuarios de PKIDEF.

Esta DPC asume que el lector conoce los conceptos de PKI, certificados y firma electrónica; en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2 *Nombre del Documento e Identificación*

La siguiente tabla de identificación aplica al presente documento:

Nombre	Declaración de Prácticas de Certificación del Ministerio de Defensa.
Versión	1.8
Estado	Revisada y Aprobada
Fecha Emisión / Fecha Caducidad	01/09/2014 Un año a partir de la fecha de emisión/ revisión del documento.
OID	2.16.724.1.1.1.1.3.0.1
Ubicación	http://pki.mdef.es/cps/cps.htm

Ilustración 1: Identificación DPC del Ministerio de Defensa

La presente DPC aplica únicamente al subconjunto de OID, soportados por la Política de Certificación del Ministerio de Defensa registrados bajo el siguiente arco de ISO/ITU-T:

id-politica-certificacion-mde ::=

{joint-iso-itu-t (2) country (16) Spain (724) administracion publica (1) minisdef (1) infocis (1) politica certificacion (1)}

Bajo dicho OID, la presente DPC soporta únicamente los siguientes niveles de confianza de los certificados, los cuales vienen definidos por los siguientes OIDs. A saber:

clase2::= {**id-politica-certificacion-mde** 2}

clase2hw::= {**id-politica-certificacion-mde** 3}

Dichas clases corresponden a los certificados en soporte software y hardware respectivamente, según se definen en la Política de Certificación del Ministerio de Defensa, según la siguiente distribución:

- **Clase 2 (OID 2.16.724.1.1.1.1.2)**, para los certificados de dispositivo o sistema con carácter general.
- **Clase 2 HW (OID 2.16.724.1.1.1.1.3)**, para certificados personales y para los elementos de la PKI (ER, EV y EST).

1.3 *Comunidad y Ámbito de Aplicación*

Se define como comunidad al colectivo de entidades a las que se proporciona certificados digitales X.509 v3 para soporte de los servicios de seguridad definidos como propósito de la Política de Certificación y contenidos en la presente DPC.

1.3.1 Autoridad de Gestión de la PKI del Ministerio de Defensa

La AGPMD es la máxima y única autoridad responsable de garantizar la correcta aplicación de la presente DPC, según la Política de Certificación del Ministerio de Defensa.

1.3.2 Entidad de Certificación

Las Entidades de Certificación que componen PKIDEF son: La Entidad de Certificación Raíz (EC-Raíz) y una Entidad de Certificación Subordinada (EC-WPG), cuyos datos, presentes en el certificado se muestran a continuación:

EC RAÍZ (EC-RAIZ)

Entidad de certificación de primer nivel. Su función es establecer la raíz del modelo de confianza de PKIDEF. Esta EC no emite certificados para entidades finales. Posee un certificado auto-firmado.

Emisor	CN = MINISDEF-EC-RAIZ OU = PKI O = MDEF C = ES
Titular	CN = MINISDEF-EC-RAIZ OU = PKI O = MDEF C = ES
Número de Serie	07 03 b1 d3 d7 ca 1c 06 08 98 8b 9e 0f 94 6c
Periodo de Validez	lunes, 13 de julio de 2009 14:21:32 viernes, 08 de noviembre de 2041 14:00:00
Función resumen del certificado.	Sha.1. f6 05 e2 3f e6 af 86 07 e4 d9 7c b8 c6 96 09 bb f0 f7 73 a8
Algoritmo de firma	sha1RSA

Ilustración 2: Identificación EC Raíz

EC SUBORDINADA (EC-WPG)

Su función es la emisión de certificados de entidad final para los subscriptores de PKIDEF.

Emisor	CN = MINISDEF-EC-RAIZ OU = PKI O = MDEF C = ES
Titular	CN = MINISDEF-EC-WPG OU = PKI O = MDEF C = ES
Número de Serie	54 14 a0 9e 80 e8 4e 73 4c 90 83 69 b1 6b e0 d2
Periodo de Validez	miércoles, 15 de septiembre de 2010 9:27:21 miércoles, 15 de septiembre de 2021 9:27:21
Función resumen del certificado.	Sha.1. e4 43 bd 00 8b c0 a9 54 5a 98 44 5d 6d 58 f7 7a b5 d5 11 9a

Algoritmo de firma	sha1RSA

Ilustración 3: Identificación EC Subordinada

1.3.3 Entidad de Registro

Las entidades de registro de PKIDEF están compuestas, de manera conjunta, por los servicios telemáticos que permiten la gestión de vida de los certificados de forma centralizada a los subscriptores y por los puestos de expedición presencial que operan en el conjunto de localizaciones dedicadas a tal fin en el territorio nacional por el Ministerio de Defensa. De esta manera, PKIDEF dispone de dos tipos de Entidades de Registro:

- Entidad de Registro Online (ER): sistema remoto que permite a los titulares de certificados personales válidos solicitar la reemisión o revocación de los mismos, de manera no presencial. También permite la solicitud remota de certificados para dispositivos y sistemas del Ministerio de Defensa a los administradores o responsables.
- Entidad de Registro Local (ERL): dedicada al registro de peticiones de certificación de los subscriptores, así como la solicitud de la reemisión o revocación de sus certificados ya emitidos, de manera presencial.

Las entidades de registro se encargarán de garantizar que la solicitud del certificado contiene información veraz y completa del Solicitante, y que la misma se ajusta a los requisitos exigidos en la presente DPC.

ER

Los servicios prestados de manera remota por la ER se identifican mediante los siguientes datos:

Emisor	CN = MINISDEF-EC-WPG OU = PKI O = MDEF C = ES
Titular	CN = MINISDEF-ER-WPG 0812.1 OU = PKI O = MDEF C = ES
Número de Serie	03 9f 19
Periodo de Validez	lunes, 12 de julio de 2010 9:37:04 jueves, 12 de julio de 2012 9:37:04
Función resumen del certificado.	Sha1.1 d8 0a 22 bd 38 16 13 5a d2 39 78 bd be 3b a0 eb 97 f2 40 c5
Algoritmo de firma	Sha1RSA.

Ilustración 4: Identificación ER-WPG 0812.1

Emisor	CN = MINISDEF-EC-WPG OU = PKI O = MDEF C = ES
Titular	CN = MINISDEF-ER-WPG 0812.2 OU = PKI O = MDEF C = ES
Número de Serie	03 9f 1b
Periodo de Validez	lunes, 12 de julio de 2010 9:39:02 jueves, 12 de julio de 2012 9:39:02
Función resumen del certificado.	Sha1.1 bd 76 18 49 b6 06 ae 7b 66 76 d5 77 6b c5 0b 6b 5b e4 f4 70
Algoritmo de firma	Sha1RSA.

Ilustración 5: Identificación ER-WPG 0812.2

Los servicios remotos ofrecidos por las ER están accesibles en la siguiente dirección:

Para los certificados de usuario: ***https://er-wpg.mdef.es:9411***

Para los certificados de dispositivos y sistemas: ***https://er-wpg.mdef.es:9410***

ERL

Las Entidades de Registro Local (ERL) son operadas por personal del Ministerio de Defensa autorizado para tal fin por la AGPMD, denominados Operadores de Registro. Las ERL no están dotadas de un certificado propio como entidad de PKIDEF, sino que son identificadas y autorizadas a través del certificado del Operador de Registro (u Operador de la ERL). La labor de una entidad de registro local (ERL) es dar soporte a las labores de la EC Subordinada, a través de un proceso de registro presencial que garantice la correcta identificación del solicitante de certificados, así como la entrega de los mismos en el momento de la solicitud.

1.3.4 Entidad de Validación.

La Entidad de Validación de certificados de PKIDEF (EV) se encarga de proveer información en tiempo real del estado de revocación de los certificados emitidos por la EC-WPG.

La Entidad de Validación realiza su labor conforme a la RFC 2560: X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol (OCSP). De esta manera la EV del Ministerio de Defensa presta servicios OCSP de forma que se pueda comprobar el estado del certificado de forma instantánea, segura y fiable. El uso del servicio de validación está autorizado a todos los usuarios (a través del componente KeyOne Desktop) y sistemas del Ministerio de Defensa, así como cualquier otra aplicación o sistema externo habilitado expresamente por la AGPMD.

La Entidad de Validación se identifica mediante los siguientes datos:

Emisor	CN = MINISDEF-EC-WPG OU = PKI O = MDEF C = ES
Titular	CN = MINISDEF-EV-WPG 0812.1 OU = PKI O = MDEF C = ES
Número de Serie	02 59 0d
Periodo de Validez	martes, 14 de julio de 2009 13:56:53 miércoles, 13 de julio de 2011 11:00:00
Función resumen del certificado.	Sha.1. c9 26 31 9d 13 4b 69 9c be 2e c3 dd b0 57 7d 91 64 36 e1 82
Algoritmo de firma	Sha1RSA.

Ilustración 6: Identificación EV

El servicio de validación se presta en la siguiente dirección exclusivamente a través del protocolo OCSP:

http://ev01-wpg.mdef.es:9308

1.3.5 Entidad de Sellado de Tiempo.

La Entidad de Sellado de Tiempo (EST) aporta evidencias criptográficas de la existencia de una determinada información o un documento electrónico en un momento determinado, el indicado por el sello de tiempo.

La Entidad de Sellado de Tiempo del Ministerio de Defensa realiza su labor conforme a la RFC 3161: Internet X.509 Public Key Infrastructure. Time- Stamp Protocol (TSP).

La EST presta sus servicios de manera exclusiva a los usuarios (a través de las herramientas de escritorio distribuidas y autorizadas por el Ministerio de Defensa en los puestos de trabajo) y sistemas del Ministerio de Defensa, no dando servicio a sistemas o aplicaciones externos al Ministerio.

Es responsabilidad de la AGPMD habilitar las aplicaciones del Ministerio de Defensa que requieran el uso de sello de tiempo y las condiciones de aplicación del mismo. La Entidad de Sellado del Tiempo no verifica la solicitud del solicitante, prestando servicio a cualquier solicitud de sello de tiempo válida que reciba a través de su servicio online. No es responsabilidad de la Subunidad de PKI implementar los mecanismos de seguridad en los puestos finales de trabajo que garanticen el envío de Sellos de Tiempo desde aplicaciones no autorizadas para ello por la AGPMD, remitiéndose a las buenas prácticas de Seguridad que apliquen a los puestos de trabajo presentes en cada ubicación del Ministerio de Defensa.

La Entidad de Sellado de Tiempo se identifica mediante los siguientes datos:

Emisor	CN = MINISDEF-EC-WPG OU = PKI O = MDEF C = ES

Titular	CN = MINISDEF-EST-WPG 0812.1 OU = PKI O = MDEF C = ES
Número de Serie	02 59 0a
Periodo de Validez	martes, 14 de julio de 2009 13:55:02 miércoles, 13 de julio de 2011 11:00:00
Función resumen del certificado.	Sha1.1. ee c2 67 bf 09 61 e3 72 1f 4b 0b b6 2a 44 b6 58 42 65 03 24
Algoritmo de firma	Sha1RSA.

Ilustración 7: Identificación EST

Así, el servicio de Sellado de Tiempo es accesible en la siguiente dirección:

http://est01-wpg.mdef.es:9207

1.3.6 Entidades relacionadas

El Directorio Corporativo del Ministerio de Defensa **(DICODEF)** proporcionará los siguientes servicios:

- Actuará de Entidad de Control de Nombres (ECN), y asignará los nombres distintivos de los titulares de certificados (Distinguished Name (DN)).
- Actuará de repositorio de información de los subscriptores de PKIDEF, de donde se extraerán los datos que serán utilizados para generar los certificados.
- Publicará la última lista de certificados revocados (CRL) generada por la EC-WPG.
- Publicará los certificados válidos emitidos para los subscriptores de PKIDEF.

Adicionalmente se requieren los servicios del servicio de mensajería corporativo (Correo Electrónico) para localizar a las entidades finales y enviar las notificaciones pertinentes, según se define en los Procedimientos de la PKI del ciclo de vida de los certificados.

También es de especial importancia la Aplicación de Gestión de Tarjetas **(AGT)**, operada en exclusiva por el personal de la Subunidad de PKI.

1.3.7 Entidades Finales

1.3.7.1 Subscriptores

A los efectos de la presente DPC, el subscriptor de los certificados de PKIDEF se corresponde con el término firmante previsto en el artículo 6 de la Ley 59/2003 de Firma Electrónica.

Un subscriptor de la PKI del Ministerio de Defensa es la entidad cuyo nombre aparece como sujeto del certificado, y que asegura que utiliza su clave y su certificado de acuerdo con la presente DPC.

La presente DPC considera como subscriptor al:

- Personal civil y militar del Ministerio de Defensa (unidades, centros y organismos) que sean notificados por el canal de comunicación pertinente a presentarse en un Puesto de Gestión de Tarjetas (PGTEMD) y posteriormente en un puesto de ERL.
- Personal civil externo que trabaja en el Ministerio de Defensa, que sean notificados por el canal de comunicación pertinente a presentarse en un Puesto de Gestión de Tarjetas (PGT) y posteriormente en un puesto de ERL.
- Estaciones de seguridad, dispositivos de red o sistemas, a saber: firewalls, servidores SSL, Controladores de Dominio, routers, switches, sistemas y aplicaciones... Estos componentes deberán estar bajo la supervisión del personal responsable de aceptar los certificados y de la correcta protección y uso de la clave privada de los mismos (denominados Agente de la PKI según la Política de Certificación). Única y exclusivamente se considerará subscriptor a un dispositivo de seguridad o sistema si este contiene en el campo mail de la entrada en el directorio la dirección de correo RFC 822 de la persona que va a administrar el mismo. Se asume la preexistencia del dispositivo o sistema en DICODEF con el nombre conforme a lo estipulado por la Entidad de Control de Nombres ECN.

Aunque las EC sean técnicamente subscriptores de PKIDEF, el término subscriptor se empleará en este documento tan sólo para aquellas entidades que soliciten certificados para usos diferentes a los de emisión y firma de certificados y CRL.

1.3.7.2 Terceros Aceptantes

Un tercero aceptante de PKIDEF, o también denominado usuario de la PKI del Ministerio de Defensa, es una entidad que utilizando el certificado de un subscriptor de la PKI del Ministerio de Defensa; verifica la integridad de un mensaje firmado digitalmente; identifica al emisor del mensaje; o establece un canal confidencial de comunicaciones con el propietario del certificado, basándose en la confianza de la validez de la relación entre el nombre del subscriptor y la clave pública del certificado proporcionada por la PKI. Un usuario de la PKI del Ministerio de Defensa utilizará la información contenida en el certificado para determinar la utilización del certificado para un uso en particular.

Los usuarios del Ministerio de Defensa sólo darán como íntegras y confiables, aquellas transacciones que vengan firmadas y validadas por otros usuarios del Ministerio de Defensa a través de los servicios de validación y sellado temporal desplegados por el propio Ministerio de Defensa o aquellos en los que se delegue.

Los usuarios del Ministerio de Defensa, en posesión de los certificados, cuya tipología describe la presente DPC harán uso sistemático de los mismos en las aplicaciones que la Autoridad Operacional del Sistema disponga para ello en cuanto su viabilidad tecnológica esté garantizada, y previa notificación y autorización de la misma por parte de la AGPMD a través de los mecanismos de comunicación pertinentes en cada centro de explotación del Ministerio de Defensa.

1.4 *Uso de los certificados*

Los certificados que se circunscriben a esta DPC deberán ser utilizados según la funcionalidad característica del perfil y el nivel de confianza bajo el que se han emitido.

PKIDEF emitirá certificados con los siguientes perfiles (clasificados según nivel de confianza):

- **Clase 2 software**: para dispositivos y sistemas cuya clave privada se haya generado en software:
  - Servidor SSL. OID 2.16.724.1.1.1.1.2.5
  - Controlador de Dominio: OID 2.16.724.1.1.1.1.2.5
  - Dispositivo: OID 2.16.724.1.1.1.1.2.5
  - Firma de Código: OID 2.16.724.1.1.1.1.2.6
  - Firma No Persona: OID 2.16.724.1.1.1.1.2.8
  - Autenticación No Persona: OID 2.16.724.1.1.1.1.2.9
  - Sede Electrónica Nivel Medio: OID 2.16.724.1.1.1.1.2.10
  - Sello Electrónico Nivel Medio: OID 2.16.724.1.1.1.1.2.14
- **Clase 2 hardware:** para personas y sistemas cuya clave privada se haya generado en un dispositivo seguro de creación de firma:
  - Autenticación Persona: OID 2.16.724.1.1.1.1.3.1
  - Firma Persona: OID 2.16.724.1.1.1.1.3.2
  - Cifrado Persona: OID 2.16.724.1.1.1.1.3.3
  - Elementos de la Infraestructura de PKIDEF: OID 2.16.724.1.1.1.1.3.4
  - Sede Electrónica Nivel Alto: OID 2.16.724.1.1.1.1.3.10
  - Autenticación Empleado Público: OID 2.16.724.1.1.1.1.3.11
  - Firma Empleado Público: OID 2.16.724.1.1.1.1.3.12
  - Cifrado Empleado Público: OID 2.16.724.1.1.1.1.3.13
  - Sello Electrónico Nivel Alto: OID 2.16.724.1.1.1.1.3.14

La descripción en detalle de cada perfil de certificado puede encontrarse en el *Anexo 2* del presente documento.

De igual manera, los certificados emitidos bajo esta DPC sólo podrán ser usados en:

- **Sistemas y aplicaciones internos** de la red de Propósito General del Ministerio de Defensa.
- **Sistemas del Ministerio de Defensa que se relacionen con ciudadanos**, según lo indicado en la Ley 11/2007 y la normativa relacionada posterior.
- **Sistemas del Ministerio de Defensa que se relacionen con sistemas externos** de otros Ministerios, Administraciones, organismos u organizaciones externas que hayan sido autorizados previamente por la AGPMD.
- **Sistemas externos** de otros Ministerios, Administraciones, organismos u organizaciones que hayan sido autorizados previamente por la AGPMD.

La expedición efectiva de los certificados soportados en la presente DPC obliga al subscriptor a la aceptación y uso de los mismos en los términos expresados en la presente DPC.

La responsabilidad en el uso de certificados digitales emitidos por PKIDEF por parte de un sistema recae en exclusividad en la Autoridad Operacional del Sistema, encargada de publicar la información que considere oportuna al respecto. Está fuera del ámbito de la presente DPC garantizar la viabilidad tecnológica de las aplicaciones que harán uso de cualquiera de los perfiles de certificados definidos en el presente documento.

1.4.1 Usos prohibidos

No se permite en modo alguno, el uso de cualquiera de los certificados fuera del ámbito descrito en la presente DPC, pudiendo ser causa de revocación inmediata de los certificados por el uso indebido de los mismos.

La presente DPC sólo permite la inserción y transporte de certificados personales emitidos por PKIDEF a los usuarios del Ministerio de Defensa en una tarjeta criptográfica TEMD.

Así mismo, la tarjeta TEMD no debe ser activada ni entregada a un usuario del Ministerio de Defensa sin sus correspondientes certificados personales.

1.5 *Gestión de la Declaración de Prácticas de Certificación*

1.5.1 Especificación de la Organización Administradora

La AGPMD es la responsable de la definición, revisión y divulgación de esta Declaración de Prácticas de Certificación (DPC).

1.5.2 Puntos de Contacto

A continuación se presentan los siguientes puntos de contacto:

- Autoridad de Gestión de la PKI del Ministerio de Defensa (**AGPMD**): Representado por el **Subdirector General de Tecnologías de Información y Comunicaciones**, con dirección de contacto: C/ Arturo Soria 289, Teléfono 91 395 4400.
- Responsable de la Subunidad de PKI: Referenciado en el presente documento como **Responsable de la Subunidad de PKI** con dirección de contacto: C/Arturo Soria 289, Teléfono 91 395 4497.
- Responsable de Seguridad Física del CCEA: Está representado por el **Jefe de la Unidad de Seguridad del CCEA** con la siguiente dirección de contacto: C/ Arturo Soria 289, Teléfono 91 395 4497.
- Entidad de Control de Nombres (**ECN**): Representado por la **Subunidad de Sistemas Medios del CCEA**, con dirección de contacto C/ Arturo Soria 289, Teléfono 91 395 4497.

1.5.3 Determinación de la aplicación de la DPC a la Política de Certificación

La AGPMD determina la idoneidad de la presente DPC con respecto a la Política de Certificación del Ministerio de Defensa.

En caso de que la Subunidad de PKI no pueda operar en las condiciones que se establecen en la presente DPC no dará servicio alguno hasta la autorización expresa de operación por parte de la AGPMD una vez estudiadas las condiciones reales de operatividad de la Subunidad de PKI.

1.5.4 Acrónimos

ACRÓNIMO	*SIGNIFICADO*
ACS	**"*A*dministrator *C*ard *S*et"**, Juego de tarjetas de administrador del módulo nCipher de uso en la reconstrucción del paradigma de seguridad de dicho módulo.
AGPMD	**A**utoridad de **G**estión de la **P**KI del **M**inisterio de **D**efensa.
AGT	**A**plicación de **G**estión de **T**arjetas
AOS	**A**utoridad **O**peracional del **S**istema.
ARL	Lista de Autoridades Revocadas (***A**uthoriry **R**evocation **L**ist*), tal como se define en la RFC 5280.
CCEA	**C**entro **C**orporativo de **E**xplotación y **A**poyo
CN	Nombre Común (***C**ommon **N**ame*)
CPS	Declaración de las Prácticas de Certificación (***C**ertificate **P**ractice **S**tatment*), tal como se define en RFC 3647.
CRL	Lista de Certificados Revocados (***C**ertificate **R**evocation **L**ist*), tal como se define en la RFC 5280.
DICODEF	**D**irectorio **Co**rporativo de **Def**ensa
DN	Nombre Distintivo (***D**istinguished **N**ame*)
DPC	Declaración de Prácticas de Certificación
EC	**E**ntidad de **C**ertificación.
ECN	**E**ntidad de **C**ontrol de **N**ombres
EGC	**E**ntidad de **G**estión de **C**ertificados: EC y ER.
ER	**E**ntidad de **R**egistro.
ERC	**E**ntidad de **R**ecuperación de **C**laves.
ERL	**E**ntidad de **R**egistro **L**ocal.
EST	**E**ntidad de **S**ellado de **T**iempo.
EV	**E**ntidad de **V**alidación del estado de los certificados.
HSM	*"**H**ardware **S**ecurity **M**odule"*

ACRÓNIMO	***SIGNIFICADO***
	Dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. Adicionalmente puede aportar aceleración hardware para operaciones criptográficas.
OCS	**"*O*perator *C*ard *S*et"**, Juego de tarjetas de operador del módulo nCipher que protege las claves de aplicación de la plataforma criptográfica de la EC Subordinada. Juego de tarjetas de operador del módulo nCipher de uso en el acceso a la información criptográfica de uso por las Entidades de la PKI de la Red de Propósito General del Ministerio de Defensa.
OCSP	"***O**nline **C**ertificate **S**tatus **P**rotocol*", Protocolo de Estado del Certificado Online, tal como se define en la RFC 2560.
PGT	**P**uesto de **G**estión de **T**arjetas.
PKCS#1	***"P**ublic **K**ey **C**ryptographic **S**yntax"* **RSA** Cryptographic Standard.
PKCS#11	***"P**ublic **K**ey **C**ryptographic **S**yntax"* Cryptographic Token Interface Standard.
PKCS#12	"***P**ublic **K**ey **C**ryptographic **S**yntax*" Personal Information Exchange Syntax.
PKI	Infraestructura de Clave Pública (*Public Key Infrastructure*)
TEMD	**T**arjeta **E**lectrónica del **M**inisterio de **D**efensa.
TSC	**T**erminal **S**eguro de **C**omunicaciones. Componente del hardware criptográfico (HSM) utilizado para introducir el pin de las tarjetas o token de administración y operación. También denominado "PIN pad"

Ilustración 8: Acrónimos

2 PUBLICACIÓN DE INFORMACIÓN Y REPOSITORIO DE CERTIFICADOS

2.1 *Repositorio de certificados*

Los repositorios de PKIDEF están compuestos por el directorio corporativo DICODEF y un servicio de publicación web.

- **DICODEF:** Accesible a través de ldap://ldap.mdef.es: 389. Configurado en Alta Disponibilidad, con una instancia maestra de escritura, en donde PKIDEF publica la información de los certificados válidos emitidos y las CRL más actualizadas, y múltiples instancias secundarias de lectura en donde se puede consultar la información.
- **Servicio de Publicación Web.** Accesible a través de http://pki.mdef.es. Permite el acceso a la información publicada por PKIDEF.

2.2 *Publicación de información*

Es obligación de PKIDEF publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados.

La presente DPC es pública y se encuentra disponible en el sitio web:

http://pki.mdef.es/cps/cps.htm

Los certificados de las EC son públicos y se encuentran disponibles en DICODEF (dentro de la rama OU = PKI, O = MDEF, C = ES) en formato X.509 v3. También se encuentran en el sitio web:

http://pki.mdef.es

La lista de certificados revocados por PKIDEF es pública y se encuentra disponible, en formato CRL v2, en DICODEF (dentro de la rama OU = PKI, O = MDEF, C = ES). También se encuentran en el sitio web:

http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl

http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl

Los certificados de los subscriptores emitidos por PKIDEF son públicos y se encuentran disponibles en DICODEF en formato X.509 v3.

- La unicidad de cada entrada en DICODEF se asume en la presente DPC por los mecanismos implantados a través de la Entidad de Control de Nombres (ECN).
- Para la emisión de un certificado se utiliza DICODEF para obtener la información necesaria para la construcción de la petición de certificación. En el momento de emitir un certificado PKIDEF comprueba que existe una entrada en DICODEF, si no fuera así, la petición de certificación sería rechazada.
- La publicación tiene lugar, para las entidades finales:
  - En la rama Personas (OU = PERSONAS, O = MDEF, C = ES) para los certificados de persona (Persona Física o Empleado Público).

- En la rama Dispositivos (OU = DISPOSITIVOS, O = MDEF, C = ES) para los dispositivos (Cortafuegos, Servidores SSL, Routers, Sedes Electrónicas y Controladores de Dominio)
- En la rama Genéricas (OU = GENERICAS, O = MDEF, C = ES) para los sistemas (Aplicaciones y Sellos Electrónicos)

2.3 *Frecuencia de publicación*

La presente DPC se **revisa una vez al año**, salvo incidencias que requieran una revisión previa, debiéndose publicar cada vez que sea modificada o actualizada.

Los certificados emitidos por PKIDEF se publican en DICODEF tras la finalización exitosa del proceso generación o reemisión, procediéndose a su eliminación automática una vez han expirado o tras su revocación. El proceso de publicación / eliminación de certificados en el repositorio se ejecuta en un período establecido de 5 minutos.

La ARL se publica de manera manual y con un periodo de **un mes**, en caso de no haber revocaciones de la EC Subordinada.

Las CRL, con un tiempo de vida de **72 horas**, se publican cada **24 horas**, procediéndose a la generación de la CRL por certificado revocado de manera inmediata, y procediéndose a su publicación en el periodo de refresco configurable de **5 minutos**.

2.4 *Protección de la publicación*

La presente DPC garantiza que el acceso a la información contenida en DICODEF desde PKIDEF tiene lugar mediante un usuario autorizado y de manera segura en las modalidades de escritura (únicamente para la EC-WPG) y lectura (resto de entidades de PKIDEF).

Para los subscriptores de la PKI el acceso de sólo lectura a la información de certificación publicada en DICODEF (acceso LDAP estándar) y el Servicio de Publicación Web (acceso HTTP estándar) es abierto.

De esta forma, el Ministerio de Defensa garantiza el empleo de sistemas fiables para los repositorios, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si el subscriptor o responsable del certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 *Registro Inicial*

3.1.1 Tipos de nombres

La EC-WPG generará y firmará certificados que contengan un nombre distintivo (Distinguished Name o DN) conforme con el estándar X.501, en el campo "SUBJECT NAME". La EC-WPG utilizará los DN de los subscriptores que les hayan sido asignados en DICODEF por la Entidad de Control de Nombres del Ministerio de Defensa.

3.1.2 Asignación de nombres

No es responsabilidad de la EC-WPG la asignación de nombres, asumiendo la existencia de los mismos en DICODEF mediante la aprobación previa de la Entidad de Control de Nombres (ECN) y los responsables del directorio.

3.1.3 Reglas para interpretar varios formatos de nombres

En todos los casos, los nombres distintivos de los certificados han de ser significativos.

La EC-WPG seguirá las reglas para interpretar los formatos de nombres establecidas por le ECN en DICODEF, basada en que los nombres distintivos de los titulares de certificados (DN) siguen la norma X.501.

3.1.4 Unicidad de los nombres

La unicidad de los nombres no está definida en la presente DPC, siendo responsable de garantizar este atributo la ECN.

3.1.5 Procedimientos de resolución de disputas de nombres

No es responsabilidad de la EC-WPG o las ER resolver sobre disputas de nombres, debiendo haber sido resueltas previamente por la ECN, que opera DICODEF.

3.1.6 Reconocimiento, autenticación y función de las marcas registradas

No estipulado.

3.2 *Validación Inicial de la Identidad*

3.2.1 Métodos de prueba de posesión de la clave privada

Cada persona que sea subscriptor de PKIDEF dispondrá de una TEMD en la que se custodiarán los certificados y claves personales del subscriptor. En un primer proceso de solicitud se opera siempre desde los puestos de Entidades de Registro Locales o ERL. En cada una de las solicitudes de certificado será el solicitante quien introduce el PIN de acceso a la tarjeta.

- El par de claves de los certificados de autenticación y cifrado se generan en formato PKCS#12 por la EC-WPG en software, a través de la librería criptográfica de la tecnología que sustenta PKIDEF. Para la generación de estos certificados se sigue un modelo centralizado. Una vez generados dichos certificados, y siempre en presencia del subscriptor que ha introducido su PIN, estos son introducidas en la tarjeta del mismo. Como medida de seguridad adicional se comprueba que la tarjeta en la que se introducen los certificados es la que tiene asignado en subscriptor.
- El par de claves del certificado de firma se generan en la tarjeta TEMD, dispositivo diseñado y fabricado con requisitos de seguridad equivalentes a una certificación Common Criteria (CC) EAL 4 PLUS, de manera que es imposible la extracción de la clave privada una vez generada a través de los atributos PKCS#11 pertinentes.
- Introducidas o generadas las claves privadas, según el caso, no se procede a comprobación adicional de posesión de clave privada, asumiendo la misma en el éxito del proceso de solicitud de certificados.
- La comunicación entre los puestos de expedición (ERL) y los servicios de la EC-WPG son cifrados y autenticados en los extremos, identificando de manera adicional al Operador de la ERL dentro del Sistema, quien firma siempre la solicitud del lote de petición de certificados.

Cuando el subscriptor es un dispositivo o sistema, el par de claves es generado por el responsable (o Agente de la PKI). Este deberá probar la posesión de la clave privada correspondiente a la clave pública que solicita que se certifique mediante el envío de la solicitud de certificación en formato PKCS#10.

3.2.2 Autenticación de la identidad de una organización

No está contemplado que PKIDEF emita certificados para personas jurídicas, por lo que no procede definir un procedimiento de identificación de las mismas.

3.2.3 Autenticación de la identidad de un individuo

3.2.3.1 Certificados de persona

3.2.3.1.1 Autenticación presencial

El proceso de **registro inicial**, para realizar la solicitud de la TEMD y sus certificados, por parte de un usuario del Ministerio de Defensa deberá realizarse presencialmente ante una Entidad de Registro Local, y presentar un documento que permita su autenticación presencial frente a PKIDEF.

Posteriormente, para cualquiera de los procesos de emisión, reemisión o revocación realizados presencialmente el subscriptor podrá personarse en una Entidad de Registro Local, y presentar un documento que permita su autenticación presencial frente a PKIDEF.

La ERL asegurará la identidad en el proceso de autenticación de la persona, para cualquier operación que esta solicite, a través de su Tarjeta de Identificación Militar (TIM), Pasaporte, Documento Nacional de Identidad (DNI), Tarjeta de Residencia o Número de Identificación de Extranjeros (NIE).

Tanto la verificación de la identidad como la propia solicitud de los certificados deberán hacerse en persona por un Operador de ERL, que haya sido designado y aprobado por la AGPMD.

Se guarda soporte escrito de tal identificación que contiene, al menos, la siguiente documentación:

- La identidad de la persona que realiza la identificación.
- Una declaración firmada de la persona que realiza la autenticación que garantice que la identidad del subscriptor se ha realizado según lo especificado en esta Declaración de Prácticas de Certificación.
- La fecha y la hora de la verificación.

En el momento de la firma de dicha copia escrita, el usuario acepta las condiciones de uso de los certificados y se somete a lo estipulado en la presente DPC en lo relativo a las condiciones de uso de los mismos.

PKIDEF autentica al Operador de ERL mediante un proceso basado en tarjeta criptográfica y verifica la autorización del mismo para operar bajo tal perfil en el sistema.

3.2.3.1.2 Autenticación electrónica remota

Se permite la autenticación electrónica ante la ER a las personas únicamente con objeto de solicitar la reemisión o revocación de todos sus certificados personales. En este caso, se solicitará la autenticación robusta mediante TEMD y el uso del certificado de autenticación del subscriptor, no permitiéndose método alternativo a esta práctica.

En posesión de un certificado de autenticación válido, en soporte TEMD, los usuarios finales del Ministerio de Defensa pueden solicitar la reemisión de sus certificados, en un número menor de tres veces, autenticándose de manera remota en el servicio:

https://er-wpg.mdef.es:9411

Una vez superado el límite que impone este contador, es obligado someterse a un proceso de reemisión presencial frente a la Entidad de Registro Local pertinente.

3.2.3.2 Certificados de dispositivo o sistema

Los dispositivos, aplicaciones y otros componentes del sistema (tales como routers, firewalls, servidores web…) deben contemplarse como subscriptores de certificados. En estos casos, el componente deberá tener asignada una persona que actúe como responsable o “Agente de la PKI”, tal y como se describe en la Política de Certificación.

El “Agente de la PKI” es el responsable de proporcionar a la ER la siguiente información:

- La identificación de los equipos.
- La información que permita gestionar los certificados del componente.
- La identificación del contacto del Agente que permita a la EC-WPG y/o ER remitirle las comunicaciones referentes al componente cuando sea necesario.

La emisión de certificados de dispositivos o sistemas se realizará previa solicitud realizada por el Agente de la PKI por alguno de los siguientes medios:

- Mediante la autenticación electrónica remota ante la ER, usando la TEMD y el certificado de autenticación del Agente. Los servicios remotos de la ER para este fin son accesibles en la siguiente dirección;

https://er-wpg.mdef.es:9411

- Mediante un correo firmado por el propio Agente PKI a la Subunidad de PKI.
- Mediante una solicitud formal a través del sistema de gestión de incidencias del Ministerio de Defensa (SCANS) a la Subunidad de PKI.

En cualquiera de estos casos, se deberá comprobar que la dirección de correo electrónico del solicitante coincide con la establecida en la entrada de DICODEF que hace referencia al dispositivo o sistema a certificar.

3.3 *Identificación y autenticación en las solicitudes de reemisión*

Se entiende por reemisión en este documento al procedimiento por el cual, un subscriptor en posesión de un certificado válido, renueva el certificado y su clave privada. La presente DPC no contempla actualmente la posibilidad de renovación simple ni la actualización de certificados. En los casos que aplicara se procederá a la revocación de los certificados y a la generación de los nuevos en las condiciones vigentes del solicitante.

3.3.1 Procedimiento de rutina para la Reemisión de un certificado

La reemisión de un certificado puede solicitarse de manera presencial en los puestos de ERL. La política de identificación y autenticación en este caso será la misma que para el registro inicial. En este caso se actualiza al valor inicial (hasta un máximo de dos) el número de reemisiones remotas a las que está autorizado un subscriptor.

En caso de solicitarse remotamente es obligatorio estar en posesión de un certificado de autenticación válido y haber realizado la operación un número menor de tres veces.

3.3.2 Procedimiento de Reemisión de un certificado después de una Revocación

El procedimiento de reemisión sólo es aplicable si el usuario posee un certificado válido del mismo tipo que se ha de renovar, de forma que la política de identificación y autenticación para la solicitud de un certificado después de una revocación será la misma que para el registro inicial.

3.4 *Identificación y autenticación en las solicitudes de revocación*

Todas las solicitudes de revocación deberán estar autenticadas.

3.4.1 Solicitud de revocación presencial

Los subscriptores, en posesión de una TEMD válida y correctamente activada, pueden solicitar la revocación de los certificados tras personarse en una ERL, debiendo aportar la razón por la que solicitan este proceso.

En caso de pérdida de tarjeta se proporcionará el número de DNI procediéndose a la revocación de todos los certificados.

El Operador de ERL, una vez que haya identificado y autenticado debidamente al subscriptor a través del DNI, Pasaporte o TIM, procesará la petición. Es deber y potestad del operador en cargo de ERL autenticar al solicitante de la revocación y juzgar la adecuación de las razones de revocación presentadas. El operador de ERL nunca procederá a la revocación efectiva en caso de detectar inconformidad con lo anteriormente expresado. En caso de disputa debe remitirse el caso a la Subunidad de PKI.

3.4.2 Solicitud de revocación electrónica remota

Los subscriptores o el Agente de la PKI, estando en posesión de un certificado de autenticación válido en su TEMD, tienen la posibilidad de solicitar la revocación de sus certificados a través del servicio:

https://er-wpg.mdef.es:9410

En este sentido, la política de identificación y autenticación se basa en la posesión de un certificado de autenticación válido, en soporte TEMD, por parte del usuario.

4 EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 *Solicitud de Certificados*

Se admitirá la solicitud de certificados personales, en soporte hardware, únicamente a aquellos usuarios finales que se presenten ante las ERL autorizadas con la carta que acredite la posesión del "PIN de Usuario" (nomenclatura específica de la AGT, responsable de la distribución del mismo) y un medio de identificación válido según lo descrito en la *sección 3.2.3* (TIM, Pasaporte, DNI, Tarjeta de Residencia o NIE). Tras las comprobaciones previas necesarias, el Operador de la ERL realizará la emisión de los certificados sobre la tarjeta TEMD.

Se admitirá la solicitud de certificados de dispositivo o sistema, en soporte software generalmente y en soporte hardware exclusivamente para certificados de Sede y Sello de Nivel Alto, a los Agentes de la PKI responsables del mismo. Un Agente de la PKI debe existir como usuario en DICODEF y figurar como administrador del dispositivo o sistema (solo se considerarán así, si en el atributo mail de la entrada en DICODEF del dispositivo en cuestión, figura la dirección de correo electrónico -formato RFC822- correcta y veraz del administrador del dispositivo o sistema. Esta condición es de cumplimiento obligado para considerar válido al Agente de la PKI según lo estipulado en la presente DPC).

No se recoge en la presente DPC la solicitud de certificado alguno fuera de la comunidad de subscriptores presentada en los párrafos anteriores.

4.1.1 Registro de las solicitudes

Para los certificados personales, el Operador de la ERL deberá establecer la identidad del subscriptor y generar un registro de solicitud. Para ello, se seguirá lo estipulado en la *sección 3.2.3*.

En el caso de certificados de dispositivo o sistema, el Agente de la PKI se autenticará frente a la Entidad de Registro Online (ER), generando él mismo el registro de solicitud, siguiendo lo estipulado en la *sección 3.2.3*.

Todas las comunicaciones entre las Entidades de Registro (ER y ERL) que dan servicio a las solicitudes y la EC-WPG que procederá a la emisión de los certificados están autenticadas y protegidas mediante mecanismos basados en claves criptográficas asimétricas (comunicaciones SSL), utilizando certificados digitales emitidos por PKIDEF.

4.1.2 Entrega de la clave pública del subscriptor al emisor del certificado

Para los certificados personales, las claves públicas de los certificados de autenticación y cifrado las genera la EC-WPG (emisor del certificado), momento en que obtiene una copia de las mismas, de manera que se considera entrega efectiva de las claves el momento de la generación de las mismas. La clave pública del certificado de firma, la genera el subscriptor en la tarjeta TEMD, recuperando la misma la EC-WPG en el momento de construcción del certificado, de manera que se considera entrega efectiva de las clave el momento de construcción del certificado. Así, las claves públicas se dan por entregadas por parte del subscriptor a la EC Subordinada (EC-WPG) en el momento de firma de aceptación de la tarjeta o PKCS#12 respectivamente.

En el caso de los certificados de dispositivos o sistemas, como regla general, el Agente de la PKI generará el par de claves (pública y privada), encargándose de su custodia y protección (puede ser en software o en un dispositivo seguro). La EC-WPG certificará la clave pública, a través de la solicitud de certificación por parte del Agente de la PKI, realizada en formato PKCS#10, devolviendo el resultado al Agente de la PKI solicitante en un fichero con formato PKCS#12. Así, las claves públicas se dan por entregadas por parte del subscriptor a la EC Subordinada (EC-WPG) en el momento de aceptación del PKCS#12.

4.2 *Tramitación de la solicitud de certificados*

La tramitación de la solicitud de certificados será realizada en las Entidades de Registro, por una persona autorizada por la AGPMD, comprobándose la identidad de los subscriptores conforme a lo establecido en el *capítulo 3* de la presente DPC.

4.3 *Emisión de Certificados*

Una vez que se reciba la solicitud de un certificado, la EC-WPG deberá:

- Verificar la identidad de la ER que gestiona la solicitud del certificado.
- Verificar los permisos de la ER y la integridad de la información de la solicitud del certificado. La ER firma las solicitudes de certificación que manda a la EC-WPG, de forma que ésta pueda comprobar la integridad de las mismas. Además, la EC-WPG posee una lista de ER permitidas, de forma que pueda comprobar que la ER solicitante posee los permisos suficientes para solicitar la certificación.
- Construir y firmar el certificado, siempre y cuando se hayan satisfecho todos los requisitos para emitir el certificado.
- Hacer que el certificado esté disponible para el subscriptor. Para ello, la EC-WPG devolverá el certificado emitido a la ER que lo solicitó por el mismo canal seguro por el que se realizó la solicitud.

Además, la EC Subordinada publica en DICODEF los certificados emitidos de forma automática con un usuario de escritura específicamente habilitado a dicho fin por la ECN.

PKIDEF no es responsable de la monitorización, investigación o confirmación de la exactitud de la información contenida en el certificado con posterioridad a su emisión. En el caso de recibir información sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, este puede ser revocado.

4.3.1 Entrega de la clave privada a los subscriptores

Para los certificados personales, las claves privadas de los certificados de autenticación y cifrado se generan en la EC Subordinada y se entregan al usuario previa introducción por parte del mismo del PIN que faculta el acceso a la parte privada de su tarjeta criptográfica TEMD en el formato seguro PKCS#12. La clave privada correspondiente al certificado de firma se genera en la TEMD del usuario previa introducción por parte del mismo del PIN que faculta el acceso a la parte privada de su tarjeta. El usuario final no debe en ningún caso aceptar otra forma de distribución de las claves privadas que la descrita en la presente DPC, debiendo siempre introducir personalmente el PIN, asegurando la confidencialidad del proceso.

4.3.2 Notificación al solicitante de la emisión por la EC del certificado

Los subscriptores son conscientes de la emisión de sus certificados al recibir su TEMD con los nuevos certificados personales.

Por otra parte, el Agente PKI será consciente de la emisión del certificado en el momento de recibir una respuesta positiva a su solicitud, recibiendo el fichero PKCS#12

4.3.3 Distribución de la clave pública de la EC a los usuarios de PKIDEF

La clave pública de la EC-WPG se distribuirá a través de su propio certificado, mediante su publicación en DICODEF y distribuyéndolo en todas las estaciones de trabajo y servidores de la WAN de Propósito General del Ministerio de Defensa mediante los mecanismos de replicación de dominio de Windows.

4.4 Aceptación de Certificados

Antes de que PKIDEF permita a un subscriptor utilizar la clave privada de su certificado, se deberá:

- Explicar al subscriptor sus obligaciones definidas en la *sección 9.6.3.*
- Informar al subscriptor que se ha generado un certificado y los contenidos del mismo.
- Requerir del subscriptor la aceptación tanto de sus obligaciones como del certificado, mediante la firma manuscrita del Documento de Aceptación[1].

La aceptación de los certificados por parte de los subscriptores se produce en el momento de la firma del Documento de Aceptación, que implica el conocimiento y aceptación por parte del subscriptor de la presente DPC y sus obligaciones.

En caso de emitir certificados de dispositivos o sistemas, los Agentes de la PKI realizarán las funciones del subscriptor.

4.4.1 Publicación del certificado por la EC

Los certificados emitidos por la EC-WPG quedarán publicados en el directorio DICODEF, en la misma rama del directorio que la establecida en el campo “SUBJECT NAME” del certificado. Los certificados quedarán publicados en el atributo “USERCERTIFICATE”.

[1] *Ver Plantillas de uso en la Entidad de Registro Local presente en el Anexo 4.*

4.4.2 Distribución de la clave pública de un subscriptor a todos los usuarios de PKIDEF

La distribución de la clave pública de un subscriptor al resto de usuarios de PKIDEF tiene lugar en el momento de la activación y generación de los certificados, que son inmediatamente publicados en la entrada de DICODEF correspondiente al Nombre Distintivo (DN) del titular.

4.5 *Uso del Par de Claves y de los Certificados*

4.5.1 Uso de la clave privada y del certificado por el subscriptor

El subscriptor, tras aceptar las condiciones de uso, sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta DPC y en la Política de Certificación del Ministerio de Defensa, y de acuerdo con lo establecido en la extensión "KEY USAGE" del certificado, especificada por el estándar X.509 v3 para la definición y limitación de tales fines. Tras la expiración o revocación del certificado el titular deberá dejar de usar la clave privada.

Los certificados regulados por esta DPC sólo se pueden utilizar con los siguientes propósitos generales:

- **Certificados de Autenticación**: autenticación frente a los sistemas del Ministerio de Defensa o externos (previamente aprobados por la AGPMD) que demanden la comprobación de la identidad del titular mediante certificado electrónico.
  - Autenticación de personas
  - Autenticación de Sedes Electrónicas
  - Autenticación de dispositivos, servidores, routers, firewalls, etc.
  - Autenticación de sistemas y aplicaciones.
  - Autenticación de controladores de dominio Windows
- **Certificado de Firma**:
  - Firma personal, firma electrónica de correos electrónicos, mensajes, ficheros y transacciones informáticas a los que se quiera dotar de control de identidad del firmante, control de integridad y no repudio.
  - Firma de Sello Electrónico para el tratamiento automatizado de la información.
  - Firma de sistemas y aplicaciones
  - Firma de componentes de código software.
- **Certificado de Cifrado**:
  - Cifrado personal, cifrado de correos electrónicos, mensajes, ficheros y transacciones informáticas a los que se quiera dotar de confidencialidad.
  - Cifrado por parte de los servidores del canal de comunicaciones.
  - Cifrado por parte de los sistemas y aplicaciones de los mensajes intercambiado o de campos parciales dentro de los mensajes.

Se puede encontrar una descripción más detallada del uso de cada perfil de certificado en el *Anexo 2* de este documento.

4.5.2 *Uso de la clave privada y del certificado por los Terceros Aceptantes*

Los Terceros Aceptantes deberán:

- Utilizar los certificados para los propósitos para los cuales fueron emitidos, tal y como se detalla en la información del certificado en la extensión "KEY USAGE".
- Comprobar que el certificado fue emitido con el OID del perfil adecuado a los propósitos para los que se quiere utilizar, tal y como se detalla en la información del certificado en la extensión "CERTIFICATE POLICIES".
- Controlar que cada certificado que se utilice es válido según lo establecido en los estándares X.509 versión 3 y la RFC 5280.
- Establecer la confianza en la EC que ha emitido el certificado, verificando la ruta de certificación de acuerdo con las recomendaciones del estándar X.509 versión 3 y la RFC 5280.

4.6 *Renovación de Certificados sin cambio de Claves (Renovación Simple)*

Según la Política de Certificación del Ministerio de Defensa se entiende por renovación simple de un certificado al procedimiento por el cual un subscriptor en posesión de un certificado válido renueva su certificado sin cambiar su clave privada.

La presente DPC no contempla el proceso de renovación simple, de forma que la renovación de claves implica necesariamente la renovación de certificado y no se pueden llevar a cabo como procesos separados.

Todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves.

4.7 *Renovación se Certificados con cambio de Claves (Reemisión)*

Según la Política de Certificación del Ministerio de Defensa, se entiende por reemisión de un certificado al procedimiento por el cual un subscriptor en posesión de un certificado válido renueva el certificado y su clave privada.

4.7.1 *Circunstancias para una reemisión*

La presente DPC establece los siguientes motivos de reemisión de un certificado:

- Expiración próxima del periodo de validez. A partir de los 3 meses antes de la caducidad del certificado, PKIDEF enviará correos de alerta al subscriptor (o al Agente PKI para el caso de los dispositivos o sistemas). Este correo de alerta se repetirá periódicamente antes de la caducidad del certificado. El envío de correos se detendrá desde el mismo momento en que se proceda a la reemisión del certificado. PKIDEF enviará el correo electrónico al subscriptor usando la dirección de correo electrónico que se encuentra publicada en DICODEF, en la entrada correspondiente al subscriptor.

4.7.2 *Quién puede pedir la reemisión de un certificado*

La reemisión debe ser solicitada por el subscriptor del certificado. En el caso de certificados de componente, el Agente de la PKI realizará las funciones del subscriptor.

4.7.3 Tramitación de las peticiones de reemisión de certificados

PKIDEF comprobará en el proceso de reemisión que la información utilizada para verificar la identidad y atributos del subscriptor es todavía válida.

La reemisión de los certificados personales se podrá solicitar:

- De forma presencial en los puestos de ERL que se establezcan, siguiendo el mismo procedimiento que en el caso de la emisión inicial. Por tanto, la identificación y autenticación para la reemisión presencial es la misma que para su emisión inicial descrito en la *sección 3.2.3.1.1*. En este caso se actualiza al valor inicial (hasta un máximo de dos) el número de reemisiones remotas a las que está autorizado un subscriptor.
- De forma remota, para lo cual es obligatorio estar en posesión de un certificado de autenticación válido y haber realizado la operación un número menor de tres veces. Por tanto, la identificación y autenticación para la reemisión remota es el descrito en la *sección 3.2.3.1.2*.

Asimismo, el procedimiento de reemisión de los certificados de dispositivo o sistema por parte del Agente de la PKI es idéntico que en el caso de la emisión inicial.

En cualquier caso la reemisión de un certificado está supeditada a:

- Que se solicite en debido tiempo y forma, siguiendo las instrucciones y normas que la presente DPC específica a tal efecto. Sólo se puede solicitar la reemisión de un certificado cada 2 años, dentro de sus últimos 3 meses de vigencia.
- Que la solicitud de reemisión se refiera al mismo tipo de certificado emitido inicialmente.
- Durante el proceso de reemisión, PKIDEF controla únicamente que el certificado esté dentro de los últimos 3 meses de vigencia y que el nuevo certificado sea del mismo tipo que el antiguo. Si ha cambiado la información relativa al subscriptor en DICODEF, se cambiarán automáticamente los datos contenidos en el nuevo certificado.

4.7.4 Notificación de la reemisión de un certificado al subscritor

Los subscriptores son conscientes de la reemisión del nuevo certificado al recibir su tarjeta TEMD con los nuevos certificados personales, si se ha realizado presencialmente, o tras la finalización del proceso automatizado de reemisión remota a través de la Entidad de Registro Online.

Por otra parte, el Agente PKI será consciente de la emisión del nuevo certificado en el momento de recibir una respuesta positiva a su solicitud recibiendo el fichero PKCS#12 correspondiente.

4.7.5 Pautas de aceptación del nuevo certificado

Las pautas de aceptación del nuevo certificado son equivalentes a las de la emisión inicial.

4.7.6 Publicación del nuevo certificado por la EC

Los certificados reemitidos por la EC-WPG quedarán publicados en DICODEF, en la misma rama del directorio que la establecida en el campo "SUBJECT NAME" del certificado. Los certificados quedarán publicados en el atributo "USERCERTIFICATE".

Para los certificados personales, los antiguos certificados son eliminados de DICODEF, de manera que sólo quedan publicados los últimos certificados válidos emitidos para el subscriptor. En el caso de dispositivos y sistemas sólo son eliminados de DICODEF los certificados expirados o revocados, pudiendo tener varios certificados válidos asociados al mismo dispositivo o sistema.

4.8 *Modificación de Certificados (Actualización)*

Según la Política de Certificación del Ministerio de Defensa se entiende por actualización de un certificado cuando alguno de los datos contenidos en el certificado deba ser cambiado. Actualizar un certificado implica crear un nuevo certificado conservando la clave privada y su validez, con número de serie diferente, y modificar al menos el valor de una extensión respecto al certificado anterior.

La presente DPC no contempla el proceso de actualización de certificados, de forma que en los casos que aplicara se procederá a la revocación de los certificados y a la generación de los nuevos en las condiciones vigentes del solicitante.

4.9 *Suspensión y Revocación de Certificados*

4.9.1 Suspensión

No se contempla la suspensión de certificados.

4.9.2 Revocación

4.9.2.1 Circunstancias para la revocación

La revocación de un certificado es el acto por el cual se deja sin efecto la validez de un certificado antes de su caducidad. El efecto de la revocación de un certificado es la pérdida de vigencia del mismo, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación. La revocación de un certificado impide el uso del mismo por parte del subscriptor.

La revocación de un certificado implica su publicación en la Lista de Certificados Revocados (CRL) de acceso público.

Las circunstancias que pueden conducir a la revocación de un certificado son:

- Que la información de identificación o de asociación de los nombres del certificado haya quedado obsoleta o sea errónea.
- Que el subscriptor deje de tener los derechos para utilizar el certificado según los términos descritos en esta DPC.
- Que quede demostrado que el subscriptor ha incumplido con sus obligaciones o esté sujeto a baja prolongada por causa mayor conforme a la normativa propia del Ministerio de Defensa o Legislación Española en vigor en el momento de aplicabilidad y vigencia de la presente DPC.
- Que exista sospecha de compromiso de la clave privada o ésta se revela como "débil".
- Que el subscriptor o el responsable de la Subunidad de PKI, pida que su certificado sea revocado.
- El certificado de una ER o EC superior en la jerarquía de confianza del certificado es revocado.
- Cese en la actividad del Ministerio de Defensa como prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos sean transferidos a otro prestador de servicios de certificación.
- Resolución judicial o administrativa que lo ordene.
- Cualquier otra aprobada en exclusividad por la AGPMD o establecida en el artículo 8 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Para cualquiera de las circunstancias descritas anteriormente se rellenará el formulario[2] correspondiente aprobado y publicado a tal fin por la AGPMD.

La revocación tiene como principal efecto sobre el certificado la terminación inmediata y anticipada del periodo de validez del mismo, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta DPC ni tendrá efectos retroactivos.

4.9.2.2 Quién puede solicitar la revocación

EC-WPG podrá revocar certificados siempre y cuando haya sido el emisor y esté autorizada la revocación por el Responsable de la Subunidad de PKI. En el caso de revocación de Entidades propias de la PKI y revocaciones masivas es potestad exclusiva de la Subunidad de PKI.

El operador de la ERL podrá solicitar la revocación del certificado de un subscriptor, en representación de las personas autorizadas para ello en la presente DPC, si tuviera la sospecha del compromiso de la clave privada del subscriptor, o cualquier otro hecho determinante que recomendara emprender dicha acción.

Los usuarios finales y Agentes de la PKI (administradores de dispositivos o sistemas) pueden solicitar la revocación de sus certificados.

En cualquier caso, la revocación de un certificado le será comunicada al subscriptor por correo electrónico, indicando el motivo de la revocación.

[2] *Ver Plantillas de uso en la Entidad de Registro Local presente en el Anexo 4.*

4.9.2.3 Procedimiento de solicitud de revocación

La EC-WPG deberá recibir una solicitud de revocación firmada, mediante uno de los siguientes procedimientos:

- El subscriptor solicita presencialmente la revocación de su certificado. El Operador de la ERL genera y firma la solicitud de revocación de un certificado en representación del subscriptor. El subscriptor rellena y firma el formulario aprobado para este fin por la AGPMD.
- El propio subscriptor solicita la revocación remota de sus certificados personales, accediendo a la ER, la cual requerirá la presentación de su certificado de autenticación. La ER comprobará que el certificado sigue siendo válido en fecha y que no haya sido revocado previamente. En este caso, la solicitud de revocación será generada y firmada por el subscriptor.
- El Agente de la PKI solicita la revocación de un certificado de dispositivo o sistema de forma remota a través de la ER. Tras la comprobación positiva de la identidad del Agente de la PKI (la ER comprobará que el certificado sigue siendo válido en fecha y que no haya sido revocado), la solicitud de revocación será generada y firmada por el Agente de la PKI en representación del subscriptor.

Cualquiera que sea el formato para realizar la solicitud de revocación deberá reflejar con exactitud el certificado que se quiere revocar, la razón por la que se solicita su revocación y facilitar la autenticación del demandante.

En particular, deberá indicarse expresamente si la revocación fuera solicitada por compromiso de clave privada o por sospecha de uso fraudulento de la misma. Cuando la solicitud la procese directamente la ER, se utilizará un formato de mensaje firmado que conozca la EC-WPG. Todas las solicitudes deberán estar autenticadas; para aquellas firmadas por el subscriptor o por la ER, con la verificación de la firma será suficiente.

La EC-WPG antes de realizar la revocación deberá comprobar la autenticidad de la petición. Queda a su criterio llevar a cabo medidas de comprobación de las razones de revocación. Si la petición de revocación es válida en forma y los motivos son coherentes, la EC-WPG revocará el certificado publicando su número de serie y demás información de identificación en la CRL, además de notificar por correo electrónico al subscriptor de la revocación del certificado y quitar el certificado del lugar donde estuviese publicado en el directorio DICODEF.

4.9.2.4 Periodo de gracia de la solicitud de revocación

Esta DPC no admite ningún periodo de gracia en la revocación de sus certificados.

La EC revocará los certificados tan pronto como valide las peticiones de revocación y siempre en el marco temporal definido en la *sección 4.9.3.1.*

4.9.2.5 Plazo en el que la EC debe resolver la solicitud de revocación

En el caso de certificados personales cuyo solicitante sea el propio subscriptor, bien presencialmente personándose ante un Operador de ERL o a través de la Entidad de Registro Online (ER), la tramitación será inmediata.

Para el resto de casos, se establece un plazo de 6 horas para la tramitación desde la notificación de la solicitud de revocación.

4.9.3 Listas de Certificados Revocados

Las listas de certificados revocados se publican en DICODEF:

cn=MINISDEF-CRL-EC-RAIZ,ou=PKI,o=mdef,c=es, para la ARL.

cn=MINISDEF-CRL-EC-WPG,ou=PKI,o=mdef,c=es, para la CRL

Las listas de certificados revocados se publican en el Directorio Activo:

cn=MINISDEF-EC-RAIZ, cn=EC-RAIZ, cn=CDP, cn=Public%20Key%20Services, cn=Services, cn=Configuration,dc=et,dc=mde,dc=es, para la ARL.

cn=MINISDEF-EC-WPG,cn=EC-WPG,cn=CDP,cn=Public%20Key%20Services, cn=Services,cn=Configuration,dc=et,dc=mde,dc=es, para la CRL

Las listas de certificados revocados se publican en un servidor web:

http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl, para la ARL.

http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl, para la CRL

En cada certificado se incorpora la dirección de la CRL, mediante la extensión cRLDistributionPoints.

4.9.3.1 Frecuencia de emisión de las CRL

Las CRL se actualizan de manera automática tras la revocación de un certificado. El tiempo de vida de una CRL será de 72 horas.

La frecuencia de emisión (y publicación inmediata) de las CRL es de 24 horas para las tipologías de Clase 2 software y hardware, aunque no se hayan producido modificaciones en la CRL, es decir, aunque no se haya revocado ningún certificado desde la última emisión.

Los certificados revocados permanecen en la CRL hasta que alcanzan su fecha de expiración. Alcanzada ésta, se eliminan de la Lista de Certificados Revocados, ante la imposibilidad de ser utilizados por estar caducados.

La ARL se publica mediante procedimientos manuales a cargo exclusivo del personal de la Subunidad de PKI, con una frecuencia mensual.

4.9.3.2 Tiempo máximo entre la generación y la publicación de las CRL

La publicación de las CRL en los repositorios es inmediata.

4.9.3.3 Requisitos de comprobación de las CRL

La verificación de la CRL es necesaria para cada uso de los certificados de entidades finales. Los terceros aceptantes deberán comprobar la validez de la CRL previamente a cada uno de sus usos y descargarse la nueva CRL de los repositorios habilitados por el Ministerio de Defensa al finalizar el periodo de validez de la que posean.

4.9.4 Disponibilidad de un sistema en línea de verificación del estado de los certificados

PKIDEF proporciona un servicio, conforme a la RFC 2560 (X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol (OCSP)) con el que los subscriptores y los Terceros Aceptantes pueden realizar la comprobación del estado de los certificados de manera online.

La EV, que proporciona el servicio OCSP está disponible las 24 horas al día para los usuarios de la PKIDEF en la localización:

http://ev01-wpg.mdef.es:9308

El servicio de validación se basa exclusivamente en consultas al estado de las bases de datos, en función de parámetros de validez configurables, de la EC-WPG de manera que se asegure una respuesta precisa del estado del certificado en el momento de su consulta.

4.9.4.1 *Requisitos de comprobación online de revocación*

Los subscriptores y los Terceros Aceptantes que deseen realizar la comprobación del estado de los certificados de manera online, deberán disponer de software capaz de operar con el protocolo OCSP, de forma que puedan obtener la información sobre el estado de los mismos.

4.9.5 Requisitos de verificación de las revocaciones por los Terceros Aceptantes

Debe realizarse la comprobación del estado de los certificados por parte de los Terceros Aceptantes. Si por cualquier circunstancia no fuera factible obtener información del estado de un certificado:

- el sistema que deba utilizarlo deberá desestimar su uso; o bien
- en función del riesgo, del grado de responsabilidad y de las consecuencias que se pudieran producir, utilizarlo sin garantizar su autenticidad en los términos y estándares que se recogen en esta DPC.

Las aplicaciones definidas para el uso con certificados en el Ministerio de Defensa comprobarán el estado de certificados preferentemente mediante protocolo OCSP.

- El uso de CRL para la verificación de los certificados sólo será admisible como método alternativo, en caso de problemas técnicos en el acceso a la Entidad de Validación o cuando el sistema trabaje de modo aislado.
- La autorización, de forma excepcional, para el uso de CRL como método exclusivo de verificación es potestad de la AGPMD.
- Si accederán sin embargo a la ARL, comprobando la validez de la misma y haciendo uso en la comprobación de la cadena de validación completa.

4.9.6 Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.10 *Servicios de comprobación de estado de certificados*

Los sistemas de consulta de la CRL y de consulta en línea del estado de los certificados (OCSP) están disponibles durante las 24 horas los 7 días de la semana para los subscriptores y para los Terceros Aceptantes.

4.11 *Finalización de la suscripción*

La suscripción (relación entre el subscriptor y la EC-WPG) finaliza con la expiración o revocación del certificado.

4.12 *Custodia y recuperación de claves*

La presente DPC sólo permite la custodia[3] y recuperación de los certificados y claves para los certificados personales de cifrado (Persona Física y Empleado Público) y nunca los empleados para la identificación del subscriptor o la firma electrónica de documentos.

La EC-WPG posee mecanismos de recuperación de claves exclusivamente para este tipo de certificados, para evitar las posibles pérdidas de información que pudiera ocasionar el olvido, extravío o compromiso de las claves utilizadas para el descifrado.

El proceso de recuperación de las claves privadas personales de cifrado requiere la expresa autorización de la AGPMD.

[3] El mecanismo técnico de generación de las claves de los certificados de autenticación en formato PKCS#12, realizado de forma centralizada por EC-WPG, exige que la EC-WPG guarde las claves (protegidas mediante cifrado) en la base de datos de PKIDEF para posibilitar su posterior entrega al subscriptor y su inserción en la TEMD. A pesar de estar almacenadas, la presente DPC no permite su recuperación en ningún caso.

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y OPERACIONALES

5.1 *Controles de Seguridad Física*

5.1.1 Ubicación y construcción

Los sistemas de información de PKIDEF se ubican en los Centros de Proceso de Datos del Ministerio de Defensa con unos niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

5.1.2 Acceso físico

El Centro de Proceso de Datos del Ministerio de Defensa (situado en el CCEA) dispone de diferentes perímetros de seguridad, con diferentes requerimientos de seguridad y autorizaciones. La presente DPC delega los controles de acceso físico a la Unidad de Operaciones de Seguridad del CCEA, Subunidad de Seguridad Física.

Las máquinas y plataformas correspondientes a los sistemas de PKIDEF, indicadas en la DPC, se encuentran etiquetadas convenientemente para su correcta identificación y ubicadas en el CPD del CCEA bajo los criterios de seguridad definidos por la Subunidad citada anteriormente.

La posesión y custodia de las llaves de acceso físico a los sistemas de PKIDEF es exclusiva del personal de la Subunidad de PKI.

5.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. El apagado de los equipos sólo se producirá en caso de fallo de los sistemas de generación autónoma de alimentación.

El sistema de acondicionamiento ambiental está compuesto por varios equipos independientes con capacidad para mantener niveles de temperatura y humedad dentro de los márgenes de operación óptimos de los sistemas.

5.1.4 Exposición al agua

Los Centros de Proceso de Datos del Ministerio de Defensa disponen de detectores de inundación y sistemas de alarma apropiados al entorno.

5.1.5 Protección y prevención de incendios

Los Centros de Proceso de Datos del Ministerio de Defensa disponen de sistemas automatizados para la detección y extinción de incendios.

5.1.6 Sistema de almacenamiento

Los soportes de información sensible se almacenan de forma segura en armarios ignífugos y cajas fuertes, según el tipo de soporte y el tipo de información en ellos contenida. El acceso a estos soportes está restringido a personal autorizado.

5.1.7 Eliminación de residuos

La eliminación de soportes magnéticos, ópticos e información en papel se realiza de forma segura.

5.2 *Controles de Procedimiento*

5.2.1 Perfiles de confianza

En general todos los perfiles definidos en PKIDEF serán exclusivamente personal de la Subunidad de PKI, no pudiendo en manera alguna solapar sus funciones en aquellos roles que se definan como excluyentes.

Los principales perfiles de confianza o roles definidos en PKIDEF son:

5.2.1.1 Administrador de Sistemas de PKIDEF

La función principal de los administradores de sistemas de PKIDEF es configurar aquellos parámetros de funcionamiento, que no afecten a la seguridad de los sistemas, de todos los componentes de PKIDEF (EC-RAIZ, EC-WPG, ER, EV y EST).

5.2.1.2 Oficial de Seguridad

Realiza la configuración de los diferentes parámetros de funcionamiento, que afectan a la seguridad de la aplicación, de todos los componentes de PKIDEF. En especial, realiza las siguientes tareas:

- Asigna roles a usuarios de PKIDEF.
- Establece los parámetros de perfiles de certificación de la EC-RAIZ y EC-WPG.
- Realiza las funciones relativas al mantenimiento de la operativa, como la publicación de las CRLs y el mantenimiento de la EC Raíz.
- Realiza la gestión de los módulos de hardware criptográfico. La operativa del módulo SafeNet Luna CA4, asociado a la EC Raíz es labor exclusiva de la Subunidad de PKI. La operativa de los OCS (Tarjetas de Operador) y ACS (Tarjetas de Administrador) correspondientes a los módulos nCipher netHSM es responsabilidad del personal de la Subunidad de PKI. No se permite responsabilidad cruzada entre los operadores de los ACS y OCS.

5.2.1.3 Oficial de Recuperación

Es el encargado de participar en el proceso de recuperación de claves de subscriptor, para los perfiles de certificados que así se haya definido en la presente DPC.

5.2.1.4 Oficial de Registro

Es el responsable de la gestión del ciclo de vida de cualquier certificado emitido por la EC-RAIZ y la EC-WPG, si bien, delega la emisión presencial de certificados a los Operadores de ERL. En especial, realizará las siguientes tareas:

- Verificar la identidad con los mecanismos y procedimientos permitidos en esta DPC.
- Registrar correctamente la identidad de los subscriptores tras su verificación.

- Asegurar las comunicaciones de peticiones y respuestas con la EC.
- La generación y revocación de certificados con la consola de la EC (EC-RAIZ o EC-WPG).
- Emitir un certificado de persona, dispositivo o sistema a través de la interfaz web de la ER.
- Acceder a la lista de certificados emitidos y revocar alguno de ellos a través de la interfaz web de la ER.
- Recibir y distribuir los certificados de los subscriptores.

5.2.1.5 *Operador de ERL*

Los Operadores de ERL serán personal designado al efecto y autorizados por el Personal de PKI del Ministerio de Defensa.

Se encargan de las funciones relacionadas con la identificación de solicitantes de certificados, la tramitación de certificados digitales, la revocación de éstos, así como la activación y el desbloqueo de tarjetas criptográficas. Los operadores de la ERL realizan y tienen bajo su responsabilidad la correcta ejecución de las siguientes acciones:

- Verificar la identidad con los mecanismos y procedimientos permitidos en esta DPC.
- Registrar correctamente la identidad de los subscriptores tras su verificación.
- Asegurar las comunicaciones de peticiones y respuestas con la EC-WPG.
- Emitir certificados personales a través de la ERL.
- Acceder a la lista de certificados emitidos y revocar alguno de ellos.
- Recibir y distribuir los certificados de los subscriptores.

5.2.1.6 *Auditor*

Posee la capacidad de acceder a cualquier elemento de PKIDEF y ver (en modo sólo lectura) todos los parámetros de la PKI, así como los ficheros de logs (trazas) generadas y los certificados emitidos.

5.2.1.7 *Operador de Sistemas Informáticos*

Es el encargado de mantener el servicio operativo de todos los componentes informáticos generales que sustentan PKIDEF: servidores, bases de datos, firewall, switches…, excluyendo el software específico de PKI y los módulos criptográficos hardware (HSM). Para ello deberán realizar las operaciones de mantenimiento que correspondan sobre los servidores y servicios de la EC-WPG.

La realización de las copias de seguridad de los datos de operación es responsabilidad del Departamento de Sistemas Medios y Bases de Datos.

5.2.1.8 *Número de personas requeridas por tarea*

Se requiere un mínimo de dos personas para establecer cualquier perfil dentro de las instalaciones de la PKIDEF.

Se requieren dos personas para la activación de claves de los dispositivos criptográficos hardware de generación y almacenamiento de claves. La modificación de los parámetros de configuración del hardware criptográfico implica la autenticación por parte de dos personas autorizadas y con privilegios suficientes.

Las EC y ER pueden ser operadas por motivos de soporte y mantenimiento por terceros contratados a tal fin y autorizados por el Responsable de la Subunidad de PKI. Cualquier operación sobre las entidades ha de ser autorizada previamente y por escrito señalando un responsable de la Subunidad de PKI que ha de velar por la correcta operativa.

5.2.1.9 *Identificación y autenticación para cada perfil*

Para acceder a las herramientas de gestión de los elementos de PKIDEF (y de la EC-WPG en particular), el usuario deberá presentar un certificado de autenticación emitido por la propia EC-WPG en tarjeta criptográfica (TEMD).

Todas las entidades autorizadas de la PKIDEF se identificarán mediante certificados digitales emitidos por la propia PKIDEF.

5.2.1.10 *Agentes de la PKI*

Los Agentes de la PKI autorizados en la presente DPC son los responsables de la administración de los siguientes tipos de elementos:

- Los administradores de los router, cortafuegos y servidores seguros (SSL).
- Los administradores de los Controladores de Dominio de Windows.
- Los administradores de las Sedes Electrónicas y Sellos Electrónicos del Ministerio de Defensa.
- Los administradores de sistemas y aplicaciones del Ministerio de Defensa.
- Aquellos componentes adicionales de seguridad de red que no estando determinados de manera específica en la presente Declaración de Prácticas de Certificación sean admitidos como de uso formal por la AGPMD en tanto soporten la solicitud de certificados en formatos PKCS#10 y la inclusión de claves privadas y cadenas de certificación en PKCS#12 de manera compatible a lo especificado en los perfiles de certificados aprobados en la presente DPC.

La nomenclatura de nombrado de los diferentes dispositivos o sistemas indicados será la definida por ECN, estando ubicados los certificados respectivos en la rama correspondiente de DICODEF y considerándose a todos los efectos subscriptores de la PKI de la WAN PG del Ministerio de Defensa según lo estipulado en la Política de Certificación.

La presente DPC solo se responsabiliza en las tareas de notificación de expiración y revocación de los certificados a aquellos dispositivos y sistemas que contengan en el atributo mail de su entrada en DICODEF la dirección de correo RFC822 correcta de su administrador.

Para emitir un certificado de dispositivo o sistema que precise de un certificado distinto de los anteriormente descritos habrá de presentarse previamente solicitud escrita y detallada ante el Responsable de la Subunidad de PKI, para analizar el perfil de certificado correspondiente y la viabilidad tecnológica en los sistemas definidos para su uso. Igualmente es potestad del Responsable de la Subunidad de PKI, denegar el uso del dispositivo si considera que la criptografía representada en el certificado no cumple los niveles mínimos para su uso en los sistemas del CCEA.

5.3 *Controles de Seguridad Personal*

El personal que se seleccione para desempeñar las funciones de control y operación de PKIDEF deberá cumplir lo dispuesto en la normativa sobre la Seguridad de la Información en las Personas (SEGINFOPER) del Ministerio de Defensa.

5.4 *Procedimientos de Control de Seguridad*

En esta sección se describen los requerimientos de seguridad de la EC y ER, incluyendo los equipos utilizados para registrar a los subscriptores y para la generación, firma, gestión y revocación de certificados.

5.4.1 Tipos de eventos a registrar

En el momento de la instalación de la EC-WPG y ER se activan los siguientes sistemas de registro de eventos (Logs), actuando estos independientemente del Nivel de Confianza y de la Clase de Certificado.

- Sistemas de Log del Sistema KeyOne PKI (software comercial que da soporte a las labores de PKIDEF), incluyendo los eventos vinculados al ciclo de vida de los certificados y las labores de administración del sistema KeyOne.
- Sistemas de Log de la Base de Datos.
- Sistemas de Log de los módulos criptográficos HSM.

Las acciones relativas a eventos y gestión de los sistemas de PKI quedan almacenadas en las bases de datos del sistema.

De esta forma, PKIDEF en general, y la EC-WPG y la ER en particular, poseen mecanismos para registrar, entre otros, los siguientes tipos de eventos:

- El acceso (logon) a las herramientas de gestión de los componentes de PKIDEF.
- La solicitud de emisión, renovación y/o revocación de certificados, por parte de la EC-WPG, registrando tanto el tipo de acción a realizar y sus parámetros, como la identificación del componente (ER), Administrador u Operador de que solicita la acción.
- Las acciones realizadas por PKIDEF. Entre ellas:
  - La generación o revocación de certificados.
  - La publicación de certificados en los repositorios.
  - La actualización de CRL y su publicación en los repositorios.
  - El envío de correos automáticos de aviso de revocación de certificados.
  - El envío de correos automáticos de aviso de caducidad próxima de certificados.
- Arranque y parada de los servicios online de los componentes de PKIDEF (y de la EC-WPG en particular).
- Los avisos (warnings) y errores producidos en el procesado de una petición por parte de la EC-WPG. Asimismo, se registrarán los avisos (warnings) y errores producidos por mecanismos internos de la EC-WPG (tales como publicación de certificados y CRL y envío de correos de aviso).

- Los intentos de acceso no autorizado a los componentes de PKIDEF, indicando la identificación de la persona que está realizando el intento.

En cada evento se registrará:

- El tipo de evento registrado.
- La fecha y hora en que se ha producido.
- La identificación del usuario o componente de PKIDEF que solicitó la acción que provocó el evento.
- El perfil o rol con el que actuó el usuario o componente de PKIDEF que solicitó la acción que provocó el evento.
- El resultado de la acción que provocó el evento.
- La descripción de la acción realizada.
- Los parámetros (contenido) de la solicitud de la acción que provocó el evento.

Toda esta información queda a disposición de los Auditores del sistema de PKI, que son las personas que pueden consultar esta información con la ayuda de las herramientas de gestión de los componentes de PKIDEF.

5.4.2 Frecuencia de procesado del registro de eventos

La frecuencia mínima de revisión de los registros es, para las Clase 2 y Clase 2 Hardware, de una vez cada 2 meses (6 veces al año), revisando al menos un 25% de los registros producidos desde la última revisión.

La información generada en los registros de eventos de PKIDEF (EC-WPG y ER) deberá almacenarse protegida hasta que la información se consolide para su revisión.

5.4.3 Periodo de retención para el registro de eventos

La información generada en los registros de eventos, salvo la generada por los HSM que utilizan repositorios locales específicos propios al igual que DICODEF y servidor de correo, se almacena en la base de datos de PKIDEF. El periodo de retención de los registros de eventos será conforme a lo especificado en la *sección 5.5.2*.

La eliminación de los registros de esta base de datos (purgado y archivado de la base de datos) se realizará por parte de un Operador de Sistemas Informáticos, que posee acceso al contenido (cifrado) y puede realizar las tareas de gestión de tablas de la base de datos. Mediante esta operación, los registros serán almacenados en un dispositivo de backup alternativo (tales como cintas magnéticas), según el periodo de retención que les aplique. Esta operación deberá ser aprobada por la AGPMD.

5.4.4 Protección del registro de eventos

Las medidas de seguridad de los registros de eventos debe garantizar que sólo las personas autorizadas pueden leerlos o eliminarlos utilizando medidas técnicas y por la implementación de procedimientos. Los procedimientos deben implementarse de manera que aseguren que no se puedan eliminar o destruir los registros de eventos antes de que haya expirado su periodo de almacenamiento.

La información de los registros de eventos se encuentra cifrada en la base de datos, de manera que sólo los Auditores pueden consultar esa información (sin capacidad de modificación) con la ayuda de las herramientas de gestión de los componentes de PKIDEF, identificándose mediante un certificado de autenticación emitido por PKIDEF y custodiado en una TEMD.

Las copias de backup de dichos registros se almacenan en un armario ignífugo cerrado dentro de las instalaciones seguras del CCEA.

La operación de limpieza de registros antiguos de la base de datos sólo se puede llevar a cabo previa autorización de la AGPMD, y almacenando previamente en un dispositivo de backup alternativo (tales como cintas magnéticas) aquellos registros que deban conservarse, según el periodo de retención que tengan estipulado.

5.4.5 Procedimientos de backup del registro de eventos

La información generada en los registros de eventos se almacena cifrada en la base de datos de PKIDEF. Se generan copias completas locales y remotas de la base de datos, de acuerdo con la Política de Copias de Seguridad del CCEA.

5.4.6 Sistema de recogida de información de eventos

Aunque forman parte de la plataforma de PKIDEF, los servicios de recogida de información de eventos se ejecutan de manera independiente de los servicios de certificación. Dicho proceso se lanza al arrancar el sistema, cesando en el momento de su apagado. Es posible disponer de los servicios de recogida de información de eventos sin necesidad de tener arrancados los servicios de certificación. No obstante, los servicios de recogida de información de eventos deben estar disponibles en el momento de arrancar los servicios de certificación, así como durante el proceso de una solicitud concreta: en caso de que los servicios de recogida de información de eventos no estén disponibles no se podrán procesar peticiones de certificación ni de revocación. En estas situaciones, la EGC seguirá recibiendo peticiones de revocación, que serán procesadas lo antes posible.

La plataforma de PKIDEF permite el funcionamiento de los servicios de recogida de información de eventos aunque no se encuentre disponible la base de datos, mediante un mecanismo alternativo de almacenamiento de registros en disco (denominados “logs de emergencia”), que serán trasladados a la base de datos cuando ésta se encuentre disponible.

5.4.7 Notificación al causante del evento

No estipulado.

5.4.8 Análisis de vulnerabilidades

La tecnología KeyOne de Safelayer dispone de mecanismos de comprobación de la integridad de los ficheros binarios y de funcionamiento de los sistemas de gestión de certificados. Todos los ficheros van firmados mediante un certificado de firma de código que emite expresamente Safelayer para el Ministerio de Defensa, cualquier fichero del sistema que no sea firmado será descartado. La Subunidad de PKI es la encargada de custodiar este certificado.

Además, en el registro de eventos quedan registrados los intentos de acceso no autorizado a los componentes de PKIDEF, indicando la identificación de la persona que está realizando el intento.

Por otra parte, el personal de la Subunidad de PKI, realiza de forma periódica un análisis de vulnerabilidades y de seguridad perimetral, constatando en todo momento la correcta actualización de los componentes que conforman PKIDEF, así como atendiendo a cualquier incidencia que en los mismos pudiera presentarse.

5.5 *Archivo de informaciones y registros*

5.5.1 Tipos de información archivada

El archivado de información de la EGC estará suficientemente detallado tanto para establecer la validez de una firma como para determinar las propias operaciones de la PKI.

Como mínimo, se archivarán los siguientes datos.

- La presente DPC, junto con sus versiones anteriores.
- La configuración del sistema, junto con sus versiones anteriores.
- Los soportes de backup de los servidores que componen la infraestructura de PKIDEF.
- Las operaciones de la EC-WPG:
  - Las peticiones de solicitud de certificados y de revocación.
  - Todos los certificados y CRL (u otra información de revocación) que se emiten o publican.
- La documentación relativa a la recepción de las tarjetas criptográficas personales TEMD (como se describe en la "*Normativa que regula los procedimiento de uso de la TEMD"*).
- La documentación relativa a la autenticación de la identidad del Subscriptor (como se describe en la *sección 3.2.3*)
- La documentación relativa a la recepción y aceptación de certificados -Documento de Aceptación- (como se describe en la *sección 4.4*).
- Los registros de eventos especificados en la *sección 5.4* de esta DPC.
- Los datos que permitan verificar los contenidos de los registros de eventos.
- Las comunicaciones relacionadas con las auditorías.

Para garantizar la recuperación y uso de la información archivada la Subunidad de PKI almacena, en una localización segura, una copia completa del software de los componentes de PKIDEF, de manera que siempre es posible recuperar los sistemas bajo los que se creó toda la información e inspeccionarla.

A nivel físico, la Subunidad de PKI garantiza la existencia de un módulo HSM SafeNet Luna CA4 y un módulo HSM nCipher NetHSM, ambos con la información criptográfica específica, que permitan la recuperación del sistema PKIDEF.

5.5.2 Periodo de retención para el archivo

Toda la información y documentación relativa al ciclo de vida de los certificados emitidos por PKIDEF se conservará durante un periodo de 15 años.

5.5.3 Protección del archivo

El acceso al archivo se encuentra restringido a personal autorizado. Asimismo, los eventos relativos a los certificados emitidos por PKIDEF se encuentran protegidos (mediante mecanismos de verificación de integridad y cifrado) en la base de datos para garantizar la detección de manipulaciones en su contenido.

La protección del almacenamiento es responsabilidad de la Unidad de Sistemas Medios del CCEA, aplicando las medidas estipuladas para el acceso y control.

5.5.4 Procedimientos de backup del archivo

Aplica la instrucción del CCEA sobre la gestión de recuperación y gestión de soporte del CCEA. Las copias de backup de dichos registros se almacenan en un armario ignífugo cerrado dentro de las instalaciones seguras del CCEA.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Los sistemas de PKIDEF realizan el registro del instante de tiempo en los que se realizan. El tiempo de los sistemas proviene de una fuente fiable de hora proporcionado por el Real Observatorio de la Armada (ROA). Todos los sistemas de PKIDEF sincronizan su instante de tiempo con esta fuente.

5.5.6 Sistema de recogida de información de auditoría (interno vs externo)

El sistema de recogida de información es interno a PKIDEF.

5.5.7 Procedimientos para obtener y verificar información archivada

Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras operaciones. La información será accedida únicamente por Auditores sobre la plataforma de PKIDEF, prohibiéndose expresamente el acceso a la misma por otro rol y otro medio que no sea el descrito en el presente párrafo. El acceso a la información únicamente tiene lugar en las plataformas autorizadas para ello de la Subunidad de PKI.

De forma automática se realizan comprobaciones de la integridad de los archivos electrónicos (backups), en tiempo de su generación y se crea una incidencia en el caso de errores o comportamientos imprevistos. En caso de querer recuperar información que haya excedido el tiempo de vida de la EC vigente, se reconstruirá el sistema de PKI correspondiente a la EC no vigente en el momento de la información que se quiera inspeccionar, procediendo a la recuperación del sistema e inspeccionando la información con el rol correspondiente, en función de la acción que se quiera realizar sobre dicha información.

5.6 *Cambio de Clave de la EC*

La validez del certificado de la EC Subordinada es de 11 años. Dado que los certificados que emite a los subscriptores poseen una validez máxima de 2 años, la EC-WPG podrá emitir certificados durante los 9 primeros años de validez. A partir de ese momento, se generará un nuevo conjunto de claves y certificados para la EC Subordinada

- Los procedimientos para proporcionar, en caso de cambio de claves, una nueva clave pública de EC a los subscriptores y Terceros Aceptantes de los certificados de la misma son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en DICODEF (ver *sección 2.1*).

5.7 *Recuperación en Caso de Compromiso de una Clave o de Desastre*

5.7.1 Alteración de los recursos hardware, software y/o datos

Si los recursos hardware, software, y/o datos se alteran o son sospechosos de haber sido alterados se detendrá el funcionamiento de los servicios de PKIDEF hasta el restablecimiento de un entorno seguro con la incorporación de nuevos componentes de eficiencia acreditable. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no reproducción de la misma.

En el caso de verse afectados certificados emitidos, se notificará del hecho a los subscriptores de los mismos y se procederá a su recertificación.

5.7.2 La clave pública de una Entidad se revoca

En el caso de la revocación del certificado de una entidad de PKIDEF (ER, EV o EST) se generará y publicará la correspondiente CRL, se detendrá el funcionamiento de la entidad y se procederá a la generación, certificación y puesta en marcha de una nueva entidad con la misma denominación que la eliminada y con un nuevo par de claves.

En el caso que la entidad afectada sea EC-WPG, se procederá a las siguientes acciones:

- Levantamiento de la EC-RAIZ, procediendo a la revocación de la EC-WPG y publicación de la ARL correspondiente.
- Posteriormente la EC-RAIZ reemitirá el certificado de la EC-WPG, el cual quedará publicado en los repositorios de información corporativos.
- El certificado revocado de la entidad permanecerá, excepcionalmente, accesible en DICODEF con objeto de permitir la verificación de los certificados emitidos durante su periodo de funcionamiento.

- Los subscriptores de PKIDEF dependientes de la entidad revocada serán informados del hecho y conminados a solicitar su recertificación por la nueva instancia de la entidad.

5.7.3 *La clave de una Entidad se compromete*

En el caso de compromiso de la clave de la EC Subordinada (EC-WPG), se procederá a su revocación inmediata según lo expuesto en el punto anterior y se informará del hecho al resto de entidades que componen PKIDEF dependientes o no de la entidad afectada, realizándose las siguientes acciones:

- Revocación masiva de los certificados generados por la EC Subordinada en el periodo comprendido entre el compromiso de la clave y la revocación del certificado correspondiente o en su totalidad si no está claro este periodo. Se procederá a la eliminación de los mismos de todos los repositorios por los mecanismos implementados en el sistema a tal fin, y en su caso si fuera necesario, con los mecanismos propios de eliminación de DICODEF y Directorio Activo.
- Publicación de la CRL correspondiente.
- Levantamiento de la EC-RAIZ, procediendo a la revocación de la EC y publicación de la ARL correspondiente.
- Posteriormente, se procederá a la generación de un nuevo certificado para la EC Subordinada.
- Los subscriptores de PKIDEF dependientes de la entidad revocada serán informados del hecho y conminados a solicitar su recertificación por la nueva instancia de la entidad.

Si la EC comprometida fuera la EC Raíz, el certificado de EC-RAIZ deberá eliminarse de todos los repositorios en los que se encuentre (punto de publicación de certificados emitidos), generar un nuevo certificado y distribuirlo de manera segura.

5.7.4 *Recuperación en caso de desastre*

El conjunto de sistemas que conforman la PKI del Ministerio de Defensa está implementado en condiciones de alta disponibilidad y redundancia en todos y cada uno de los componentes que lo conforman. De esta manera se garantiza la continuidad de los servicios frente a caída de cualquiera de sus componentes. De manera añadida, se contempla el uso de un Centro de Respaldo o secundario, que daría continuidad de dichos servicios frente a catástrofe o mantenimientos de las instalaciones que albergan el sistema primario.

En el caso de una indisponibilidad de las instalaciones de la Entidad de Certificación EC-WPG por un periodo superior a veinticuatro horas, la presente DPC remite al uso del Plan de Contingencia del CCEA vigente a tal fin.

5.8 *Cese de una EC*

Las causas que pueden producir el cese de la actividad de la Entidad de Certificación son:

- Compromiso de la clave privada de la EC, en cuyo caso se actuará según lo establecido en las *secciones 5.7.2 y 5.7.3* de esta DPC.
- Decisión organizativa por parte del Ministerio de Defensa.

En caso de cese de su actividad como Prestador de Servicios de Certificación, el Ministerio de Defensa realizará, con una antelación mínima de dos meses, las siguientes acciones:

- Informar a todos los subscriptores de sus certificados y extinguir la vigencia de los mismos revocándolos.
- Comunicar al Ministerio competente en materia de Sociedad de la Información y firma electrónica el cese de su actividad y el destino que va a dar a los certificados, así como cualquier otra circunstancia relevante relacionada con el cese de actividad.
- Remitir al Ministerio competente en materia de Sociedad de la Información y firma electrónica toda la información relativa a los certificados electrónicos revocados para que éste se haga cargo de su custodia.

6 CONTROLES DE SEGURIDAD TÉCNICA

Los componentes de la arquitectura de la PKI del Ministerio de Defensa están todos acreditados por las normas de seguridad aplicables, siendo, de manera adicional, objeto de desarrollos y adecuaciones específicas del ámbito de seguridad del Ministerio de Defensa.

6.1 *Generación e Instalación del Par de Claves*

6.1.1 Generación del par de claves

Las claves de la EC Raíz se generan y custodian en un módulo criptográfico SafeNet Luna CA4, dispositivo certificado FIPS 140-2 nivel 3.

Las claves de la EC-WPG (o EC Subordinada) se generan y custodian en módulos criptográficos nCipher NetHSM 1600 y Thales nShield Connect 1500, siendo estos dispositivos criptográficos certificados FIPS 140-2 alcanzando globalmente el nivel 3. Adicionalmente los módulos Thales nShield Connect 1500 poseen la certificación Common Criteria (CC) con nivel EAL4+.

Las claves de las Entidades de Validación, Sellado de Tiempo y Entidades de Registro son generadas y custodiadas en los módulos nCipher NetHSM 1600 y Thales nShield Connect 1500.

La clave de los usuarios en tarjeta, perfil de firma, tiene lugar en la propia tarjeta TEMD, aceptada para su uso en el Ministerio de Defensa y diseñada originalmente con requisitos de seguridad equivalentes a una certificación CC EAL4+.

Las claves para los Sellos Electrónicos de Nivel Alto y las Sedes Electrónicas de Nivel Alto se generarán en módulos SafeNet Luna SA, siendo este un dispositivo criptográfico certificado FIPS 140-2 alcanzando globalmente el nivel 3. Adicionalmente los módulos SafeNet Luna SA poseen la certificación CC EAL4+. Todos los dispositivos seguros SafeNet Luna SA HSM proporcionan las más altas garantías como dispositivos seguros de creación de firma electrónica, cumpliendo con los perfiles de protección establecidos en la especificación técnica CEN:CWA 14167.

Las claves de los usuarios, para los perfiles de autenticación y cifrado, se generan a través de software de forma centralizada, haciendo uso del motor criptográfico de la herramienta KeyOne de Safelayer, si bien el proceso de solicitud de números aleatorios se delega a los dispositivos nCipher.

En general, cuando el subscriptor es un dispositivo o sistema (excepto los ya comentados Sede y Sello de Nivel Alto), el par de claves es generado por el responsable (o Agente de la PKI) en software, utilizando la herramienta más adecuada según el modelo de dispositivo, servidor, aplicación o sistemas (IIS, Java, Apache, Cisco IOS…). Es obligación del Agente de la PKI el custodiar de forma segura las claves generadas. Posteriormente, el envío de la solicitud de certificación a la EC-WPG se hará en formato PKCS#10.

6.1.2 Entrega de la clave privada a los subscriptores

Ver la *sección 4.3.1, Entrega de la clave privada a los subscriptores*.

Para los certificados personales, las claves privadas se generan en presencia del subscriptor, si bien únicamente la de firma se genera en la tarjeta sin que sea extraída. Las claves de autenticación y cifrado se generan centralizadamente por PKIDEF y se insertan a través de un PKCS#12 en la tarjeta.

En el caso de los certificados de dispositivos o sistemas, como regla general, el Agente de la PKI generará el par de claves (pública y privada), encargándose de su custodia y protección (puede ser en software o en un dispositivo seguro).

6.1.3 Entrega de la clave pública al emisor del certificado

Ver la *sección 4.1.2*, *Entrega de la clave pública del subscriptor al emisor del certificado.*

Las claves públicas generadas por medios bajo el control de los usuarios finales se envían a PKIDEF como parte de una solicitud de certificación en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

6.1.4 Distribución de la clave pública de la EC a los terceros aceptantes

Los subscriptores reciben la clave pública de la EC mediante los mecanismos detallados en la *sección 4.3.3*, Distribución de la clave pública de las EC a los usuarios de PKIDEF.

Por otra parte, los terceros aceptantes podrán descargar los certificados confiables desde los repositorios identificados en la *sección 2.1*.

6.1.5 Longitud de las claves

La longitud de las claves RSA es 4096 bits para la EC Raíz (EC_RAIZ).

La longitud de las claves RSA es 2048 bits para la EC Subordinada (EC-WPG), EST, ER y EV.

La longitud de las claves RSA es 2048 bits para los certificados personales en TEMD (Persona Física y Empleado Público).

La longitud de las claves RSA es 2048 bits para los certificados de Sede Electrónica Nivel Alto y Sello Electrónico Nivel Alto.

La longitud de las claves RSA es 1024 bits para los certificados de dispositivo (incluida Sede Electrónica de Nivel Medio) y de sistema (incluido Sello Electrónico de Nivel Medio) en software.

Las claves de ofuscación específicas del sistema KeyOne son claves RSA de longitud 1024 bits.

6.1.6 Parámetros de generación de la clave pública

Los parámetros de clave pública son generados conforme a PKCS#1, utilizándose como segunda pareja de la clave pública, **FERMAT 4**[4].

6.1.7 Comprobación de la calidad de los parámetros

La calidad de los parámetros en el módulo criptográfico SafeNet Luna CA4 de la EC Raíz (EC-RAIZ) es garantizada por la certificación FIPS 140-2 nivel 3.

[4] El n-ésimo número de Fermat es $F_n=(2)^{(2^n)}+1$.

La calidad de los parámetros en los módulos criptográficos nCipher NetHSM 1600 de la EC Subordinada (EC-WPG), ER, EV y EST es garantizada por la acreditación FIPS 140-2 nivel 3.

La calidad de los parámetros en el módulo criptográfico SafeNet Luna SA es garantizada por la acreditación FIPS 140-2 nivel 3.

La calidad de los parámetros en la Tarjeta TEMD, con tecnología de Microelectrónica, es garantizada por el cumplimiento de un nivel de seguridad equivalente a CC EAL4+.

6.1.8 Hardware / software de generación de claves

Las claves correspondientes a los certificados de las entidades de PKIDEF están custodiadas en dispositivos criptográficos seguros (HSM), cumpliendo la certificación FIPS 140 Nivel 3.

La tarjeta criptográfica utilizada para almacenar los certificados personales es la TEMD que cumple un nivel de seguridad equivalente a CC EAL4+. Todos los números aleatorios necesarios para la generación de las claves de los certificados personales se generan en los HSM o las tarjetas criptográficas.

Las operaciones criptográficas en software para los certificados de dispositivo y sistemas las realizará el Agente de la PKI a través de la librería criptográfica más adecuada al uso previsto para el certificado.

6.1.9 Fines del uso de la clave

El uso de las claves viene indicado en la extensión “KEY USAGE” y “EXTENDED KEY USAGE” de los certificados.

En la presente tabla se muestra el conjunto de usos de las claves según la tipología de aplicación del certificado:

Certificado	KEY USAGE	EXTENDED KEY USAGE	CRÍTICA
AUTENTICACIÓN (PERSONA FÍSICA / EMPLEADO PÚBLICO)	digitalSignature	clientAuth, emailProtection, smartCardLogon	Uso de clave Restricciones básicas
FIRMA PERSONA (PERSONA FÍSICA / EMPLEADO PÚBLICO)	nonRepudation	NO USADO	Uso de clave Restricciones básicas
CIFRADO (PERSONA FÍSICA / EMPLEADO PÚBLICO)	KeyEncipherment DataEncipherment	clientAuth, emailProtection	Uso de clave Restricciones básicas
SEDE ELECTRÓNICA	digitalSignature KeyEncipherment	serverAuth	Uso de clave Restricciones básicas
SELLO ELECTRÓNICO	digitalSignature nonRepudiation keyEncipherment dataEncipherment	clientAuth, emailProtection	Uso de clave Restricciones básicas
SERVIDOR SSL,	digitalSignature	serverAuth	Uso de clave

DISPOSITIVO	KeyEncipherment		Restricciones básicas
CONTROLADOR DE DOMINIO	digitalSignature KeyEncipherment	clientAuth, serverAuth	Uso de clave Restricciones básicas
FIRMA NO PERSONA	digitalSignature keyEncipherment dataEncipherment	clientAuth, emailProtection	Uso de clave Restricciones básicas
AUTENTICACIÓN NO PERSONA	digitalSignature KeyEncipherment keyAgreement	clientAuth	Uso de clave Restricciones básicas
FIRMA DE CÓDIGO	digitalSignature	codeSigning	Uso de clave Restricciones básicas

Ilustración 9: Fines del uso de la clave

6.2 *Protección de la Clave Privada*

6.2.1 Estándares para los módulos criptográficos

El módulo SafeNet Luna CA4 de la EC Raíz (EC-RAIZ) cumple con la certificación FIPS 140-2 nivel 3.

Los módulos nCipher NetHSM 1600 del resto de entidades de la PKI (EC-WPG, ER, EST y EV) y el módulo SafeNet Luna SA cumplen con la certificación FIPS 140-2 nivel 3.

Las tarjetas criptográficas TEMD cumplen cumple un nivel de seguridad equivalente a CC EAL4+.

Todos los dispositivos mencionados anteriormente soportan el estándar PKCS#11.

6.2.2 Control multipersona de la clave privada

En caso de certificados personales, el acceso a las claves privadas está protegido mediante PIN. En este caso el acceso se realizará por una única persona, el propio subscriptor.

Por otra parte, los certificados de dispositivo o sistema emitidos en software deben ser custodiados por el Agente de la PKI. La presente DPC no establece el control multipersona a estos certificados, dejando la responsabilidad al Agente PKI.

Las claves correspondientes a los certificados de las entidades de PKIDEF (EC-RAIZ, EC-WPG, ER, EST y EV) residen custodiadas en dispositivos criptográficos seguros (HSM), en los cuales hay definidos esquemas de control multipersona para la activación y acceso de las claves privadas. Estos mecanismos son dependientes del modelo de HSM utilizado.

- El acceso a la clave privada de la EC Raíz está sujeto a un proceso de autenticación basado en token de seguridad. Cada token es intransferible y están segmentados en perfiles de operación específicos en la Subunidad de PKI.

- El acceso y puesta en marcha del módulo SafeNet Luna CA4 de la EC Raíz requiere la autenticación mediante token del Usuario de Seguridad del dispositivo, perteneciente también a la Subunidad de PKI. Para poder realizar estas acciones, el módulo ha de recuperarse previamente de la caja fuerte situada en las instalaciones seguras de la Subunidad de PKI a través del Responsable de la Subunidad de PKI o del llavero autorizado. El llavero es el operador actual del TSC del SafeNet Luna CA4 o sustituto del responsable de la Subunidad de PKI con acceso a la caja fuerte en las instalaciones seguras.
- El acceso a cualquier clave privada de los módulos nCipher NetHSM 1600 que dan servicio a la EC Subordinada está protegido por un juego de tarjetas de memoria (OCS) custodiado de manera personal e intransferible por al menos dos miembros de la Subunidad de PKI.

La presente DPC admite que el conjunto de operadores de seguridad de la EC Raíz no tenga por qué ser necesariamente disjunto del conjunto de operadores de la EC subordinada.

6.2.3 Custodia de la clave privada

Las claves privadas correspondientes a los certificados personales serán custodiadas en la tarjeta criptográfica TEMD del subscriptor, estando protegido el acceso a las operaciones con las mismas mediante PIN.

- En concreto, las claves de no repudio son generadas y custodiadas en la TEMD no permitiendo su exportación, de forma que sólo los subscriptores custodiarán la única copia de esta clave.
- Las claves privadas de los certificados de autenticación[5] y cifrado se generan centralizadamente por PKIDEF, insertándose con posterioridad en la tarjeta TEMD en formato PKCS#12, previa introducción del PIN por parte del usuario.
- La presente DPC sólo permite el procedimiento de recuperación (previa copia de seguridad y custodia por parte de PKIDEF) de las claves privadas de los certificados personales de cifrado (Persona Física y Empleado Público), para evitar las posibles pérdidas de información que pudiera ocasionar el olvido, extravío o compromiso de las claves utilizadas para el descifrado.
- La copia de las claves privadas de los certificados personales de cifrado se encuentran protegidas a nivel físico en el CPD, lugar donde están ubicados los sistemas de almacenamiento, y lógico (mediante técnicas criptográficas) por los sistemas dedicados a tal fin de la plataforma KeyOne de Safelayer, operada por la Subunidad de PKI.

El cambio de PIN de la TEMD del usuario está permitido y únicamente puede realizarse en la siguiente dirección:

https://srvcceaagtw01.mdef.es/AGT/agt

[5] El mecanismo técnico de generación de las claves de los certificados de autenticación en formato PKCS#12, realizado de forma centralizada por EC-WPG, exige que la EC-WPG guarde las claves (protegidas mediante cifrado) en la base de datos de PKIDEF para posibilitar su posterior entrega al subscriptor y su inserción en la TEMD. A pesar de estar almacenadas, la presente DPC no permite su recuperación en ningún caso.

Las claves privadas para los certificados de dispositivo o sistema generadas en software deberán ser custodiadas de forma segura por el Agente de la PKI.

Por tanto, la custodia de la clave privada, independientemente del soporte, es responsabilidad del subscriptor, accediendo a la misma mediante PIN o contraseña segura.

Las claves correspondientes a los certificados de las entidades de PKIDEF (EC-WPG, ER, EST y EV) residen custodiadas en dispositivos criptográficos seguros (HSM).

- La custodia del conjunto de claves privadas de la EC Raíz, generadas y contenidas en el módulo SafeNet Luna CA4 tiene lugar en la Subunidad de PKI a nivel físico y lógico. El acceso requiere un proceso de autenticación seguro basado en token de seguridad.
- La custodia del conjunto de claves privadas de la EC Subordinada y del resto de entidades de la PKI tiene lugar en la Subunidad de PKI a nivel lógico y CPD a nivel físico. El acceso requiere un proceso de autenticación múltiple basado en tarjeta de memoria en el paradigma de seguridad de los módulos criptográficos respectivos.

6.2.4 Copia de seguridad de la clave privada

Para la EC Raíz, en todo momento existe una copia de seguridad en soporte físico de las claves privadas, procediéndose a su revisión cada **año**, y procediendo a la creación de una **nueva copia cada dos años**. Pasado el primer año, solo convivirán dos copias de respaldo, procediendo a eliminar, frente a entrada de una nueva la más antigua en caso de aplicar.

Para las claves del resto de entidades de PKIDEF (EC-WPG, ER, EST y EV), en todo momento existe una copia de seguridad en soporte físico de los parámetros de definición del "Mundo Seguro"[6], que contiene las referencias a las claves de operador, administrador y del sistema de la PKI. Así mismo, se incluye copia de las referencias a las claves. Se procede a su revisión **mensual**, procediéndose a la creación de una nueva copia cada tres meses. Pasado los **seis** primeros meses, solo convivirán dos copias de respaldo, procediendo a eliminar frente a entrada de una nueva la más antigua en caso de aplicar. En caso de modificar cualquier parámetro que afecte al "Mundo Seguro" o a las claves del sistema se procede de manera inmediata a la creación física de la copia sin que se proceda la destrucción de la anterior y manteniendo el ciclo de vida de dicho respaldo. Esto obedece a la necesidad de recuperar en un momento dado situación preexistente.

Se permite a los Agentes de la PKI que reciban certificados de dispositivo o sistema de clase 2 software realizar copias de seguridad de los ficheros PKCS#12 entregados por PKIDEF.

[6] Componente específico de la tecnología de nCipher crítico para la coherencia de los módulos criptográficos y recuperación posterior de su entorno de seguridad e información criptográfica.

La presente DPC sólo permite el procedimiento de recuperación (previa copia de seguridad y custodia por parte de PKIDEF) de certificados personales para la tipología de cifrado (Persona Física y Empleado Público), para evitar las posibles pérdidas de información que pudiera ocasionar el olvido, extravío o compromiso de las claves utilizadas para el descifrado. La copia de seguridad de las claves privadas de los certificados personales de cifrado será realizada por PKIDEF, de esta manera se puede proceder a la recuperación de las mismas a través del servicio de recuperación de claves, el cual es operado en exclusividad por el personal de la Subunidad de PKI:

- El proceso de custodia de las claves privadas de los certificados personales de cifrado están sujetos a los procesos de copia de respaldo y recuperación del sistema de bases de datos.
- El proceso de recuperación de las claves privadas personales de cifrado requiere la expresa autorización de la AGPMD.
- El proceso de recuperación de las claves privadas de cifrado requiere el exitoso cumplimiento de un proceso de autenticación de, al menos, dos operadores de recuperación de claves basado en contraseña a través de la consola de administración de la Entidad.
- El servicio de recuperación de claves está presente y disponible en la siguiente localización, pudiendo acceder al mismo los operadores de recuperación de claves habilitados en la Subunidad de PKI de forma específica a tal fin a través de su certificado de autenticación:

https://ec-wpg.mdef.es:9109/

La operativa con cualquier clave privada está restringida de manera única y exclusiva al personal de la Subunidad de PKI designado a tal fin, no permitiéndose en ningún caso la operativa de los sistemas que albergan las mismas a terceros.

6.2.5 Archivo de la clave privada

Las copias de backup de las claves privadas de los componentes de PKIDEF se almacenan cifradas en la caja fuerte situada en las instalaciones seguras de la Subunidad de PKI.

Las copias de backup de las claves privadas de los certificados personales de cifrado, sujetas a los procesos de copia de respaldo y recuperación de bases de datos, se almacenan cifradas en armarios seguros ignífugos.

6.2.6 Introducción de la clave privada en el módulo criptográfico

La generación de las claves privadas de los componentes de PKIDEF siempre tiene lugar en los HSM, no permitiéndose bajo ninguna circunstancia la introducción de material alguno en los módulos que no sea material específico de la PKI del Ministerio de Defensa. La detección de material criptográfico adicional distinto del mencionado dará lugar a la suspensión inmediata de los servicios de la EC-WPG hasta resolución de la incidencia.

Para los certificados personales, las únicas claves que se introducen en las tarjetas TEMD son las correspondientes a los certificados de autenticación y cifrado, siendo la clave privada de firma generada de manera local en las tarjetas. La inclusión de material adicional criptográfico en las tarjetas está estrictamente prohibida, salvo expresa autorización por parte de la AGPMD, y la detección del mismo dará lugar a la revocación inmediata de los certificados y eliminación de dicha tarjeta a través de los sistemas de revocación de PKIDEF y gestión de tarjetas respectivamente.

6.2.7 Método de activación de la clave privada

En caso de certificados personales, el acceso a las claves privadas está protegido mediante PIN, que deberá ser conocido sólo por el propio subscriptor.

La clave privada tanto de la EC-RAIZ como de la EC-WPG se activa mediante la inicialización del software de EC y la activación del hardware criptográfico que contiene las claves.

- La activación de la clave privada de EC-WPG tiene lugar siempre bajo palabra de paso o contraseña de un miembro de la Subunidad de PKI, al cual está asignada la custodia de una tarjeta OCS de los módulos nCipher. Esta palabra siempre se introduce sin visibilidad de la misma.
- La activación de las claves privadas del SafeNet Luna CA4 tiene lugar previa introducción del PIN de activación que está en posesión del Responsable de Seguridad, o en su defecto del llavero designado, a través del TSC del dispositivo. De manera adicional, la activación en el sistema de PKI tiene lugar de a través de un proceso de autenticación múltiple basado en tarjeta criptográfica bajo un protocolo de desafío respuesta.

6.2.8 Método de desactivación de la clave privada

Se puede proceder a la desactivación de la clave de las Entidades de Certificación de PKIDEF mediante la detención del software de EC.

6.2.9 Método de destrucción de la clave privada

En caso de proceder a la destrucción de una clave privada del módulo SafeNet Luna CA4 se hará a través de la herramienta de administración propia de SafeNet.

En caso de proceder a la destrucción de una clave privada de algún módulo nCipher NetHSM 1600, se llevará a cabo a través de la herramienta de administración de nCipher, previa autenticación del operador de seguridad correspondiente.

Las claves serán borradas mediante el proceso de puesta en modo fábrica, que garantiza el borrado total y seguro de las claves en cualquiera de los módulos. No se procede en ningún caso a la destrucción de las tarjetas de Operador y Sistema, ni a la destrucción de los registros locales, ya que son críticos para la reconstrucción del sistema si fuera necesario. Se excluye cualquier otro método en la presente DPC que no sean los que implementan los propios módulos criptográficos.

No se contempla en esta DPC la destrucción física de un HSM en ningún caso

Para el caso de la tarjeta criptográfica TEMD se procederá al reinicio únicamente del dispositivo, no procediéndose en caso alguno al borrado de los registros de seguridad de las claves de cifrado personales almacenadas en PKIDEF. El proceso siempre debe ser precedido por una revocación de los certificados asociado a la tarjeta.

La destrucción de una tarjeta criptográfica, cuando pierda su validez, deberá realizarse de forma segura y a nivel físico.

6.3 *Otros Aspectos de la Gestión del par de Claves*

6.3.1 Archivo de la clave pública

Las claves públicas quedan almacenadas en los sistemas de archivado de PKIDEF, como parte del proceso de archivo de los certificados, un periodo de quince (15) años.

6.3.2 Periodo de uso para las claves públicas y privadas

Los certificados de entidad final (personales, de dispositivo y de sistemas), así como sus pares de claves asociados, tienen un periodo de uso de dos (2) años, si bien en el momento de su emisión la EC-WPG puede establecer excepcionalmente periodos inferiores.

El certificado de EC-RAIZ tiene una validez de treinta y seis (36) años, el de EC-WPG de once (11) años, y el del resto de entidades de PKIDEF (ER, EV y EST) de dos (2) años.

6.4 *Datos de Activación*

6.4.1 Generación y activación de los datos de activación

En caso de certificados personales, el acceso a las claves privadas está protegido mediante PIN, que deberá ser conocido sólo por el propio subscriptor. Para la tarjeta TEMD el PIN de activación de los datos cumple con las especificaciones FIPS 112: tiene una longitud mínima de 6 caracteres, de los cuales al menos hay dos alfabéticos, uno al menos en mayúsculas, siendo el resto numérico.

Los datos de activación de las EC y otros componentes de PKIDEF se generan y almacenan en tarjetas criptográficas en posesión del personal autorizado de la Subunidad de PKI.

6.4.2 Protección de los datos de activación

Ningún subscriptor podrá difundir por motivo alguno, ni almacenar en soporte alguno, el PIN de activación, ya sea de su tarjeta criptográfica personal o módulo criptográfico, esto es, juegos de tarjeta de operador y administrador, o token del Usuario de Seguridad del módulo SafeNet Luna CA4.

En cuanto a los componentes físicos de activación de los HSM, estos están sujetos a los mecanismos de seguridad disponibles en la Subunidad de PKI.

6.4.3 Otros aspectos de los datos de activación

No estipulado.

6.5 *Controles de Seguridad Informática*

Las buenas prácticas de seguridad y uso en los puestos informáticos de trabajo, está fuera del alcance de la presente DPC. El Responsable de la Subunidad de PKI es quien vela por la correcta ejecución de dichas prácticas por parte del personal de su Departamento.

La gestión física y lógica de las máquinas que albergan la plataforma de PKI es responsabilidad de la Subunidad de PKI. Cualquier operativa física o lógica sobre dichas plataformas debe ser aprobada previamente por el Responsable de la Subunidad de PKI quien estará informado en todo momento de operaciones externas sobre dichas plataformas. Es potestad de dicho responsable la denegación del acceso a las plataformas debiendo arbitrar la AGPMD la resolución de posibles disputas.

El acceso lógico a las plataformas que soportan los servicios de la PKI de la WAN de Propósito General del Ministerio de Defensa tiene lugar mediante un usuario específico definido a tal fin. La gestión completa del ciclo de vida de dicho usuario es responsabilidad y uso exclusivo en su totalidad de la Subunidad de PKI del Ministerio de Defensa. El acceso de este usuario[7] a los sistemas tiene lugar mediante palabra de paso a través de los sistemas de acceso remoto seguro autorizados a dicho fin por la Subunidad de PKI. El acceso a las plataformas no proporciona permisos de administrador o root.

Por otra parte, las aplicaciones informáticas de gestión de PKIDEF, requerirán la presentación de un certificado de autenticación almacenado en tarjeta TEMD, custodiado por los propios administradores de PKIDEF. Cada acceso será almacenado en el registro de eventos de PKIDEF. Una vez autenticado, el administrador podrá realizar las operaciones permitidas a los roles que tenga asignados.

6.6 *Controles de Seguridad del Ciclo de Vida*

Los desarrollos y personalizaciones de productos implementados que gestionan el ciclo de vida de los certificados del Ministerio de Defensa se han realizado siguiendo de manera exhaustiva los controles de seguridad establecidos por la AGPMD y conforme a lo requerido en la Política de Certificación del Ministerio de Defensa, en lo expuesto y relativo a las clases de certificados contemplados en la presente DPC.

En general, se deberá contemplar lo siguiente:

- En los equipos en que se realicen las funciones de la EC, sólo se podrán instalar las aplicaciones o componentes de software que están en relación con la configuración identificada para realizar las funciones definidas para la EC.
- De forma análoga, y siempre que sea posible, en los equipos que soporten la funcionalidad de la ER, EV y EST tampoco se instalarán aplicaciones o componentes de software externos a la configuración identificada para realizar las funciones definidas para estos componentes.
- De la misma forma, siempre que sea posible, los puestos de Operadores de ERL serán estaciones de trabajo dedicadas a esa labor, y no será instalado ningún software externo a la configuración identificada para realizar las funciones definidas para la ERL.

[7] Dicho usuario tiene capacidad de operación sobre los servicios de PKI del Sistema KeyOne v3 y sobre los módulos criptográficos nCipher netHSM 1600. No tiene sin embargo permisos de administrador sobre la plataforma y las bases de datos que soportan los datos de producción y registro de la PKI de la WAN PG del Ministerio de Defensa.

Cualquier actualización o cambio del hardware y/o software de los componentes de PKIDEF se llevarán a cabo por personal especializado y autorizado por la AGPMD.

6.7 *Controles de Seguridad de la Red*

La red de aplicación está protegida por cortafuegos que solo permiten el tráfico autorizado entre los distintos componentes de PKIDEF. Así, los flujos de información que tienen lugar entre los distintos elementos de la plataforma están dados de alta en la configuración de los cortafuegos. Asimismo, están presentes y activados sistemas de seguridad adicionales, que garantizan la detección de eventos potenciales que pudieran suponer una brecha de seguridad.

Adicionalmente, los puestos de los Operadores de ERL también están debidamente dados de alta y autorizados, de manera que se controla también los lugares origen del tráfico pudiéndose impedir el acceso de dichos puestos al entorno de explotación de los servicios de PKIDEF.

El personal a cargo de la correcta configuración y uso de dichos sistemas es personal de la Subunidad de PKI.

6.8 *Controles de Seguridad de los Módulos Criptográficos*

Los requerimientos para los módulos criptográficos se describen en la *sección 6.2.1.*

7 PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRL)

7.1 *Perfil de Certificado*

7.1.1 Número de versión

Los certificados emitidos por PKIDEF siguen el estándar X.509 versión 3 (X.509 v3).

7.1.2 Extensiones del certificado

Las extensiones utilizadas en los certificados, de forma genérica, son:

- **KeyUsage.** Calificada como crítica.
- **BasicConstraint.** Calificada como crítica.
- **CertificatePolicies.** Calificada como no crítica.
- **SubjectAlternativeName.** Calificada como no crítica.
- **CRLDistributionPoint.** Calificada como no crítica.

En el Anexo 2 del presente documento se recogen los perfiles de los certificados de entidad final que emite PKIDEF.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Las firmas de los certificados emitidos bajo esta política se identifican con los siguientes OIDs:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62(10045) signatures(4) 1}

Así mismo, los certificados contendrán los siguientes OIDs para identificar los algoritmos de las claves públicas emitidas:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type(2) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

La PKI del Ministerio de Defensa sólo certificará las claves públicas asociadas con los algoritmos criptográficos identificados anteriormente, y sólo utilizará los algoritmos criptográficos de firma descritos anteriormente para firmar certificados, listas de certificados revocados y cualquier otro producto de PKIDEF.

7.1.4 Formatos de nombres

Los certificados emitidos por PKIDEF contienen el Distinguished Name X.500 del emisor y el del destinatario del certificado en los campos "ISSUER NAME" y "SUBJECT NAME" respectivamente.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names (DN) X.500, únicos y no ambiguos.

Los atributos CN "COMMON NAME" y OU "ORGANIZATION UNIT" del DN serán los que distingan a los DN entre sí. El resto de atributos tendrán los siguientes valores fijos: O=MDEF, C=ES

No está definido en la presente DPC imponer restricciones en los nombres que no estén conformes con lo definido por la Entidad de Control de Nombres (ECN).

7.1.6 Identificador de objeto (OID) de la Declaración de Prácticas de Certificación

PKIDEF, a través de la AGPMD, tiene definida una política de asignación de OID dentro del arco privado de numeración correspondiente al Ministerio de Defensa. De esta forma, el OID de todos los perfiles de certificados de PKIDEF comienzan con el prefijo **2.16.724.1.1.1.1.** Los certificados emitidos bajo esta DPC, sólo utilizarán los OID identificados para su clase, esto es, Clase 2 en soporte software y Clase 2 en soporte hardware.

Ver *sección 1.2.*

7.1.7 Uso de la extensión "Policy Constraints"

No estipulado.

7.1.8 Sintaxis y semántica de los calificadores de política

La extensión "CERTIFICATE POLICIES" contiene los siguientes calificadores de política ("Policy Qualifiers"):

- **"CPS POINTER":** reservada para contener la URI de la presente DPC y la Política de Certificación que rigen el certificado.
- **"USER NOTICE":** Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

Dentro del *Anexo 2* se puede ver su contenido para los certificados regulados por esta DPC.

7.1.9 Tratamiento semántico para la extensión "Certificate Policy"

Esta DPC requiere que la extensión "CERTIFICATE POLICIES" esté marcada como no crítica. Esta extensión se interpretará de acuerdo a la RFC 5280.

7.2 *Perfil de CRL*

7.2.1 Número de versión

Las CRL emitidas por PKIDEF siguen el estándar X.509 versión 2 (X.509 v2).

7.2.2 CRL y extensiones

7.2.2.1 ARL de la Entidad de Certificación Raíz

Los campos y extensiones autorizados en la presente DPC son los siguientes:

Campo	Contenido	Critica
Versión	V2	
Signature		
AlgorithmIdentifier		
Algorithm	SHA-1WithRSAEncryption (1:2:840:113549:1:1:5)	
Parameters	Solo se incluirán en el caso de usar Id-dsa-with-sha-1	
IssuerName	CN= MINISDEF-EC-RAIZ, OU=PKI O=MDEF, C=ES	
ThisUpdate	Fecha de emisión	
NextUpdate	30 días desde la fecha de emisión	
revokedCertificates		
userCertificate		
CertificateSerialNumber	Entero que indica al certificado que está siendo revocado	
RevocationDate	Fecha de revocación	
crlEntryExtension		
ReasonCode	No utilizado	NO
certificateissuer		SI
CrlExtensions		
authorityKeyIdentifier	Derivada de utilizar la función hash sha-1 sobre la clave pública de la EC emisora	NO
issuerAltName	No utilizado	NO
CrlNumber	Entero. Número que se incrementa secuencialmente	NO
issuingDistributionPoint		NO
onlyContainsUserCerts	BOOLEAN. A falso por defecto	NO
onlyContainsCACerts	BOOLEAN. VERDADERO	
IndirectCRL	BOOLEAN. A falso por defecto	
DeltaCRLIndicator	Esta extensión solo debe aparecer en el caso de ser una deltaCRL	SI

Campo	Contenido	Critica
BaseCRLNumber	Este valor será igual que el CRLNumber	

Ilustración 10: ARL

7.2.2.2 *CRL de la Entidad de Certificación Subordinada*

Los campos y extensiones autorizados en la presente DPC son los siguientes:

Campo	Contenido	Critica
Versión	V2	
Signature		
AlgorithmIdentifier		
Algorithm	SHA-1WithRSAEncryption (1:2:840:113549:1:1:5)	
Parameters	Solo se incluirán en el caso de usar Id-dsa-with-sha-1	
IssuerName	CN= MINISDEF-EC-WPG, OU=PKI O=MDEF, C=ES	
ThisUpdate	Fecha de emisión	
NextUpdate	Tiempo de vida de la CRL 72 horas. Se emite una nueva CRL (si no hay revocaciones) cada 24 horas.	
revokedCertificates		
userCertificate		
CertificateSerialNumber	Entero que indica al certificado que está siendo revocado	
RevocationDate	Fecha de revocación	
crlEntryExtension		
ReasonCode	No utilizado	NO
Certificateissuer		SI
CrlExtensions		
authorityKeyIdentifier	Derivada de utilizar la función hash sha-1 sobre la clave pública de la EC emisora	NO
issuerAltName	No utilizado	NO
CrlNumber	Entero. Número que se incrementa secuencialmente	NO
issuingDistributionPoint	Esta extensión no debe ser crítica para permitir el “smartcardlogon” en Windows	NO
onlyContainsUserCerts	BOOLEAN. VERDADERO	NO
onlyContainsCACerts	BOOLEAN. A falso por defecto	
IndirectCRL	BOOLEAN. A falso por defecto	
DeltaCRLIndicator	Esta extensión solo debe aparecer en el caso de ser una deltaCRL	SI

Campo	Contenido	Critica
BaseCRLNumber	Este valor será igual que el CRLNumber	

Ilustración 11: CRL

8 AUDITORÍA DE CONFORMIDAD

8.1 *Frecuencia de los controles de conformidad para cada entidad*

Se llevará a cabo una auditoría sobre los componentes de PKIDEF, al menos una vez al año, para garantizar la adecuación de su funcionamiento y operativa con las disposiciones incluidas en esta DPC.

8.2 *Identificación / cualificación del auditor*

El auditor de seguridad deberá ser independiente, a nivel organizativo, de PKIDEF, y no deberá pertenecer en ningún caso a la Subunidad de PKI, encargada de la administración y operación de las entidades de PKIDEF.

Los auditores deberán tener la adecuada capacitación y experiencia en PKI, seguridad, procesos de auditoría y tecnologías criptográficas, además de un exhaustivo conocimiento de la presente DPC. Al menos uno de los auditores deberá poseer formación sobre la administración y operación del software con el que se implementa PKIDEF (KeyOne del fabricante Safelayer).

Se permite en la presente DPC la contratación de personal externo especializado para la realización de los controles de auditoría mediante la fórmula contractual de aplicación en el Ministerio de Defensa.

8.3 *Relación entre el auditor y la entidad auditada*

Al margen de la función de auditoría, el auditor y la parte auditada (PKIDEF) no deberán tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses.

El auditor demandará el acceso al sistema con el rol específico de Auditor. En las labores de inspección que quiera llevar a cabo en relación a los módulos criptográficos HSM, estos serán siempre operados por el personal de la Subunidad de PKI, proporcionando al mismo la información requerida. El auditor no estará en ningún caso autorizado a la manipulación física de los HSM, ni se le suministrará acceso a las máquinas que soportan la plataforma de PKIDEF. En caso de realizar auditoria de los niveles de seguridad física, será siempre acompañado por el personal de la Subunidad de PKI.

8.4 *Aspectos cubiertos por el control de conformidad*

La auditoría determinará la conformidad de los servicios de PKIDEF con esta DPC y la Política de Certificación del Ministerio de Defensa. También determinará los riesgos del no cumplimiento de la adecuación con la operativa definida por esos documentos. Se procederá a auditar, como mínimo, los siguientes aspectos considerados críticos:

- Adecuación de la presente DPC a la Política de Certificación del Ministerio de Defensa.
- Adecuación de las medidas efectivas y controles técnicos existentes en PKIDEF con los procedimientos marcados en la presente DPC.
- Adecuación de PKIDEF con lo establecido en la Política de Seguridad de la Información del Ministerio de Defensa (Orden Ministerial 76/2006).

- Medidas efectivas de seguridad en el acceso a la administración y roles de las distintas entidades que conforman la PKI
- Revisión de los procedimientos de administración y operación de los servicios de la EC-RAIZ y EC-WPG.
- Segregación efectiva de los roles establecidos en la presente DPC.
- Evaluación de los niveles de seguridad física.
- Evaluación tecnológica:
  - Control y seguimiento de las versiones de software y correcta actualización del mismo, procediendo a la comprobación del software en explotación y las versiones oficiales soportadas por la plataforma.
  - Revisión de las capacidades de espacio de las máquinas que conforman las entidades del PKI de cara a prevenir desbordamientos de espacio.
- Revisión de los procedimientos de contingencia, así como la capacidad efectiva del personal de la Subunidad de PKI.
- Revisión de las copias físicas de respaldo del contenido de los módulos criptográficos HSM, y del estado de las bases de datos de los sistemas de PKIDEF.
- Validez del origen de los usuarios que dan de alta a los distintos operadores de las ERL y los operadores de la AGT en cualquiera de los roles. Esto es, se debe asegurar que los operadores de cualquier entidad han sido dados de alta tras las autorizaciones pertinentes, siguiendo lo estipulado en la presente DPC y siempre por personal competente para ello.

De manera genérica, conjuntamente con los aspectos críticos señalados anteriormente se procederá a auditar conforme a las buenas prácticas definidas en ISO27001.

8.5 *Acciones a tomar como resultado de una deficiencia*

Si se encuentra una deficiencia, se llevarán a cabo las siguientes acciones:

- El auditor realizará un informe con los resultados de su auditoria.
- El auditor notificará la deficiencia a las partes identificadas en la *sección 8.6*.
- La Subunidad de PKI propondrá las acciones correctivas para solucionar la deficiencia, indicando el tiempo estimado para su aplicación a la AGPMD.
- Una vez que la deficiencia sea subsanada, será necesario realizar una nueva auditoría para confirmar su implantación y la efectividad de las soluciones tomadas.

En caso de una deficiencia grave la AGPMD determinará la solución más adecuada, pudiendo llegar a la suspensión temporal de las operaciones de PKIDEF hasta que las deficiencias se corrijan, a la revocación del certificado de una entidad, cambios en el personal,…

8.6 *Comunicación de resultados*

El auditor comunicará los resultados de la auditoria a la AGPMD.

Asimismo, serán comunicados a la Entidad auditada de la plataforma, así como a los responsables de las distintas áreas en las que se detecten problemas.

9 REQUISITOS COMERCIALES Y LEGALES

9.1 *Tarifas*

No se estipula ninguna tarifa aplicable a la prestación de servicios de certificación o revocación por parte del Ministerio de Defensa en la presente DPC.

9.2 *Capacidad financiera*

El Ministerio de Defensa dispone de garantía de cobertura suficiente de responsabilidad civil a través de un seguro de caución que cubre el riesgo de la responsabilidad por los daños y perjuicios que pudiera ocasionar el uso de los certificados expedidos por su PKI, cumpliendo así con la obligación establecida en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

9.3 *Política de Confidencialidad*

9.3.1 Información sensible que debe protegerse

Se declara expresamente como información sensible, que no podrá ser divulgada a terceros, excepto en aquellos supuestos previstos legalmente:

- Las claves privadas de las entidades que componen PKIDEF.
  - Se protege mediante los medios físicos presentes en la Subunidad de PKI la información criptográfica que conforma el acceso a la EC Raíz.
  - Se protege el acceso a las tarjetas de Operación y Administración de los módulos criptográficos que dan soporte a la EC Subordinada, así como los números de serie y de activación de los soportes criptográficos hardware.
  - Se protege a través de las buenas prácticas de la Subunidad de PKI del Ministerio de Defensa, las palabras de paso que garantizan el acceso seguro a las plataformas de gestión y operativa de la EC Subordinada y demás entidades que conforman la plataforma actual de PKIDEF.
- Las claves privadas de cifrado de subscriptores de las que PKIDEF mantenga en custodia.
- Toda información relativa a las operaciones que lleve a cabo PKIDEF.
- Toda información relativa a los parámetros de seguridad, control y procedimientos de auditoría.
- Toda la información de carácter personal proporcionada a PKIDEF durante el proceso de registro de los subscriptores de certificados
- Planes de continuidad de negocio y de emergencia.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

9.3.2 Información no sensible

La AGPMD considera información de acceso público:

- La contenida en la Declaración de Prácticas de Certificación aprobada por la AGPMD.
- Los certificados emitidos así como las informaciones contenidas en éstos.
- La lista de certificados revocados (CRL)

Se permite el acceso a la información considerada no sensible, sin perjuicio de que se establezcan los controles de seguridad necesarios con el fin de evitar que puedan añadir, modificar o suprimir contenidos por personas no autorizadas.

9.3.3 *Divulgación de información de revocación de certificados*

La información relativa a la revocación de certificados se proporciona vía CRL en los repositorios autorizados, así como a través de la Entidad de Validación a través del protocolo OCSP.

9.4 *Protección de datos personales*

De acuerdo con el artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, toda información de carácter personal proporcionada a PKIDEF por los subscriptores de sus certificados será tratada de acuerdo con los términos de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

La información personal que se incluye en los certificados es obtenida en su totalidad del directorio corporativo del Ministerio de Defensa (DICODEF). Aquellos datos que son proporcionados adicionalmente durante la solicitud de los certificados o en el momento de la comprobación de la identidad del subscriptor (en los términos que se prevén en el artículo 17.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica), se obtienen con el consentimiento de los titulares.

En ningún caso PKIDEF incluye en los certificados electrónicos que expide, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

PKIDEF sólo podrá comunicar informaciones calificadas como sensibles o que contengan datos de carácter personal en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

9.4.1 *Responsabilidades*

El Ministerio de Defensa garantiza el cumplimento de sus obligaciones legales como prestador de servicios de certificación, de conformidad con la Ley 59/2003, de 19 de diciembre, y en virtud de esto, y de acuerdo con los artículo 22 y 23 de dicha Ley, responderá por los daños y perjuicios que cause en el ejercicio de la actividad que le es propia.

9.5 *Derechos de Propiedad Intelectual*

Todos los derechos de propiedad intelectual, incluyendo los referidos a certificados y CRL emitidos por PKIDEF, OIDs, la presente Declaración de Prácticas de Certificación, la Política de Certificación, así como cualquier otro documento, electrónico o de cualquier otro tipo, propiedad de PKIDEF, pertenecen y permanecerán en propiedad del Ministerio de Defensa.

9.6 *Obligaciones y Responsabilidad Civil*

Se detallan a continuación las obligaciones de la comunidad de usuarios destacados en la presente DPC.

9.6.1 Obligaciones de la Entidad de Certificación

La Entidad de Certificación Subordinada de la WAN de Propósito General del Ministerio de Defensa (EC_WPG) actuará relacionando unas determinadas claves públicas con el subscriptor a través de la emisión de los certificados personales, todo ello de conformidad con los términos de esta DPC y de la Política de Certificación del Ministerio de Defensa.

La EC-RAIZ y EC-WPG, en los procesos de gestión del ciclo de vida de los certificados y control de las tarjetas, tienen las siguientes obligaciones:

- Realizar sus operaciones en conformidad con esta DPC.
- Proteger sus claves privadas.
  - Incorporan mecanismos de control de acceso basado en roles, que requieren, si así se exige, la autenticación múltiple de los operadores correspondientes.
    - En la EC Subordinada el conjunto de grupos que requieren un proceso de autenticación múltiple son los siguientes: Operadores de Recuperación de Claves, Operadores de Revocación de operadores de ERL y Operadores de Revocación Masiva.
    - En particular, para los Operadores de Revocación Masiva se requiere de manera explícita y obligada que al menos uno de los Operadores no pertenezca a la Subunidad de PKI, debiendo ser designado por la AGPMD. La presencia de dicho operador es obligada en caso de deberse proceder a dichas operaciones. El Responsable de la Subunidad de PKI, en caso de necesidad justificada, podrá autorizar la ejecución de dicha acción sin contar con dicho operador, notificándose de manera inmediata a la AGPMD la justificación de la acción y siempre tras haber recibido autorización en soporte electrónico o de papel para la ejecución de la acción.
    - Así mismo, los Operadores que operan la EC Raíz realizan la autenticación frente a los componentes de PKI basándose en tarjeta criptográfica. Estos operadores realizan una autenticación previa frente al módulo criptográfico de uso exclusivo por la EC Raíz. Por el impacto de las Operaciones, en la EC Raíz, salvo el rol de Auditor, todos los roles pertenecen a un grupo múltiple siendo disjuntos dos a dos.
  - Discriminan roles específicos para la gestión y uso de los módulos criptográficos que la soportan en la generación, custodia y destrucción segura de las claves.

  - El Usuario de Seguridad del SafeNet Luna CA4, módulo criptográfico de la EC Raíz realiza la gestión de los token y del TSC para la puesta en marcha operativa del SafeNet Luna CA4, dando paso de manera posterior a los distintos perfiles que operen la EC Raíz. La presente DPC no inhabilita que un mismo Operador de la EC Raíz ostente el cargo de Usuario de Seguridad del módulo SafeNet. El llavero físico del SafeNet Luna CA4 corresponde al Responsable de Seguridad de la Subunidad de PKI, permitiéndose el uso de las mismas a un miembro de la Subunidad de PKI específicamente nombrado a tal fin. En ningún caso se permitirá ninguna operación de la EC Raíz a personal civil o militar, que no sea miembro de la Subunidad de PKI y esté asignado a tal fin.
  - A tal efecto, la administración de los módulos criptográficos de la EC Subordinada y entidades asociadas se basa en división de roles a la cual aplica los mismos criterios que los mencionados anteriormente. En ningún caso se permite que un miembro de la Subunidad de PKI sea simultáneamente Usuario de Seguridad del módulo SafeNet Luna CA4 y custodio de las ACS del nCipher, no aplicando la presente restricción al conjunto de tarjetas OCS del módulo de la EC Subordinada.
- Emitir certificados ajustándose a los perfiles, tanto de certificados como CRL, descritos en esta DPC y en la Política de Certificación del Ministerio de Defensa.
- Tras la recepción de una solicitud válida de certificado, emitir certificados conformes con el estándar X.509 y con los requerimientos de la solicitud.
- Asegurar que la información de registro se acepta por la ER y los puestos de ERL, los cuales están obligados a cumplir con esta DPC.
- Incluir sólo la información válida y apropiada en el certificado, y guardar evidencias de que se han seguido los procedimientos aprobados para su validación.
- Garantizar la confidencialidad en el proceso de generación de datos de creación de firma y su entrega por un procedimiento seguro al solicitante.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
- Garantizar que puede determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió su vigencia.
- Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

- Revocar los certificados en los términos de la *sección 4.9* y publicar los certificados revocados en la CRL en los servicios de directorio y servicio web referidos en la *sección 2.1*, con la frecuencia estipulada en la *sección 4.9.3*.1
  - PKIDEF procede a la revocación del certificado, eliminándolo de DICODEF y publicando de manera inmediata la CRL actualizada, de manera que se garantiza la consistencia de la información presente en DICODEF.
- Utilizar los servicios de repositorio que satisfagan las obligaciones reflejadas en la *sección 2.1*
- Asegurar que las obligaciones que se imponen a los subscriptores son las reflejadas en la *sección 9.6.3* de la presente DPC, y que se les informará de las consecuencias del incumplimiento de las mismas.
- Conservar los Documentos de Aceptación de condiciones de uso de los certificados personales firmados, en papel o electrónicamente, con los solicitantes de certificados en los que estos se dan por enterados de sus obligaciones y derechos, consienten en el tratamiento de sus datos personales por la EC y confirman que la información proporcionada es correcta.
- Publicar esta DPC en el sitio web http://pki.mdef.es/cps/cps.htm
- Garantizar la disponibilidad de las CRL de acuerdo con las disposiciones de la *sección 4.9.4* de la presente DPC.
- En el caso de que la EC proceda a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con lo establecido en el presente documento y en la Política de Certificación.
- Operar de acuerdo con la legislación aplicable. En concreto con:
  - La Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
  - La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.
  - La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Proteger las claves bajo su custodia.
- No almacenar en ningún caso los datos de creación de firma, clave privada, de los subscriptores de certificados emitidos con el propósito de utilizarse para firma electrónica.
- En caso de cesar en su actividad, comunicarlo con una antelación mínima de dos meses al cese efectivo, a los titulares de los certificados emitidos, así como al Ministerio de Industria, Turismo y Comercio, comunicando el destino que va a dar a los certificados.
- Cumplir las especificaciones contenidas en la normativa sobre Protección de Datos de Carácter Personal.
- Conservar registrada toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento durante quince años desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.

- Autenticar todos los extremos de las comunicaciones, cifrando el canal, garantizando la correcta identificación y autenticación de los dos extremos de las comunicaciones.
- Dar soporte de manera segura a los distintos servicios que se requieren desde las otras entidades de PKIDEF (ER, EV, EST).
- Incorporar los mecanismos de seguridad física presentes en las instalaciones del CCEA, garantizando la seguridad física del conjunto de sistemas que conforman la PKI del Ministerio de Defensa.
- Mantener procedimientos de copia de respaldo, y redundancia en los componentes y servicios de manera que se garantiza la continuidad del servicio de forma ininterrumpida.

Toda EC que actúe en discrepancia con estas obligaciones estará sujeta a las acciones que se contemplan en la *sección 8.5* de esta DPC.

9.6.2 Obligaciones de la Entidad de Registro Local.

La ER y los puestos de ERL de PKIDEF deben cumplir las siguientes obligaciones:

- Realizar sus operaciones en conformidad con esta DPC.
- Identificar correctamente al subscriptor, conforme a los procedimientos que se establecen en esta DPC, utilizando cualquiera de los medios admitidos en derecho.
- Informar, antes de la emisión de un certificado, a la persona que solicite sus servicios, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de dispositivos de creación y de verificación de firma, de las condiciones para la utilización del certificado, y de la página web donde puede consultar cualquier información relativa a PKIDEF.
- Formalizar la generación y expedición de certificados con el subscriptor en los términos y condiciones establecidas en la presente DPC.
- No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.
- Recibir y tramitar las solicitudes de revocación presenciales que reciba de manera inmediata, después de haber llevado a cabo una identificación fiable del solicitante.
- Solicitar la revocación de un certificado cuando tenga conocimiento o sospecha del compromiso de una clave privada.
- Formalizar el Documento de Aceptación con el subscriptor según lo establecido por esta DPC.
- Almacenar de forma segura, y hasta su remisión a la AGPMD, la documentación aportada en el proceso de emisión del certificado y en el proceso de revocación del mismo.
- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta DPC.

El puesto de ERL, o ER, que no cumplan con estas obligaciones estará sujeto a la revocación de su operativa.

9.6.2.1 Particularidades de la ERL

Una Entidad de Registro Local (ERL) está operada en exclusividad por el personal designado a dicho fin por el Responsable de la Unidad donde estén ubicadas. Para adquirir el rol de operador de ERL es necesario realizar un periodo de formación específico (descrito en el documento Instrucción Técnica "IN-344-CCEA/SE/01/09/V1" de Constitución y Funcionamiento de los Puestos de Gestión de la Tarjeta Electrónica del Ministerio de Defensa). Los nuevos operadores serán dados de alta en los sistemas de PKIDEF únicamente por la Subunidad de PKI, previa autorización del Responsable de la Subunidad de PKI y de la AGPMD.

Las ERL han de notificar al Responsable de la Subunidad de PKI, la dirección IP de las máquinas desde las que prestan servicios para que esta sea dada de alta en los sistemas de seguridad de comunicaciones de la Subunidad de PKI.

Las máquinas que soporten las ERL son de propósito exclusivo a dicho fin, no debiéndose instalar en ningún caso software que no sea estrictamente necesario para la operativa de los servicios ofrecidos por las ERL.

Los Operadores de las entidades de registro local, únicamente solicitan la petición de certificados en soporte hardware, previa autenticación del solicitante vía DNI, TIM, Pasaporte, Tarjeta de Residencia o NIE. Los Operadores de la ERL no admitirán en ningún caso otro documento de identificación que los descritos anteriormente. Los Puestos de ERL únicamente proporcionan certificados clase 2 hardware en tarjeta TEMD para personal civil o militar a través, únicamente, del proceso de generación de certificados.

Los Operadores de ERL, una vez generados los certificados e insertados en la tarjeta, proporcionarán a firmar al solicitante un Documento de Aceptación[8] que especifica la fecha de emisión. En ese momento el solicitante pasa a ser subscriptor, aceptando plenamente las prácticas de comportamiento y uso de los certificados descritos en la presente DPC.

Las ERL prestan su servicio en habilitaciones del Ministerio de Defensa, llevando a cabo las buenas prácticas y usos correctos de seguridad que se determinen en cada caso en lo referente a la seguridad física de los puestos de trabajo e instalaciones. Es deber del Responsable de Seguridad de los puestos de trabajo asegurar que dichas condiciones se lleven a cabo, deteniendo la operativa de las ERL y elevando en su caso y si procede queja a la AGPMD y notificando el cese de las operaciones al Responsable de la Subunidad de PKI.

El Responsable de la Subunidad de PKI, puede bajo sospecha fundada de una operativa incorrecta de un operador de las ERL ordenar y ejecutar la baja inmediata del operador de la ERL e impedir el tráfico entre dicha ERL y los servicios de PKI, procediendo a la notificación de las causas y acciones llevadas a cabo a la AGPMD. La operativa no se restablecerá hasta la resolución de las incidencias, previa notificación y autorización de inicio de las actividades por parte del Responsable de la Subunidad de PKI.

[8] *Ver Plantillas de uso en la Entidad de Registro Local presente en el Anexo4.*

9.6.2.2 Particularidades de la ER.

La Entidad de Registro online será operada en exclusividad por el personal designado para tal fin por el Responsable de la Subunidad de PKI. Dichos operadores serán dados de alta en el Sistema de PKIDEF únicamente por personal de la Subunidad de PKI, previa autorización del Responsable de la Subunidad de PKI.

Las máquinas desde las que se accede a las funcionalidades de administración de la ER están ubicadas de manera exclusiva en las instalaciones de la Subunidad de PKI.

La Entidad de Registro online guarda registro de todas las operaciones realizadas, garantizando en todo momento la reconstrucción de las acciones que permiten el conocimiento completo de las circunstancias en que se solicita la revocación. Cuando se procede a la revocación de un certificado, se realiza la publicación inmediata de una nueva CRL en los repositorios autorizados a través de los mecanismos habilitados en PKIDEF.

Finalmente, la ER garantiza a los usuarios en posesión de una tarjeta TEMD válida y en posesión de un certificado de autenticación vigente la renovación automática de los certificados que ya posee el usuario, en las condiciones de seguridad estipuladas en la presente Declaración de Prácticas de Certificación.

9.6.3 Obligaciones de los subscriptores

Las obligaciones de los subscriptores son:

- Suministrar a las Entidades de Registro (ER o ERL) información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.
- Hacer uso de los certificados a través de las aplicaciones habilitadas para ellos por el Ministerio de Defensa.
- Poner el cuidado y medios necesarios para garantizar la custodia de su clave privada, evitando su pérdida, divulgación, modificación o uso no autorizado.
- Garantizar la privacidad de su palabra de paso o PIN, cumpliendo las políticas de conformación de su contraseña en el momento de su paso de solicitante a subscriptor.
- Notificar de manera inmediata, a la ER o a la EC que haya proporcionado el certificado la sospecha de compromiso de clave o su pérdida, robo o deterioro. Esta notificación deberá realizarse de manera presencial en la ERL emisora o a través del servicio telemático de la ER.
- Atenerse a todos los términos, condiciones y restricciones exigidos en el uso de sus claves privadas y certificados.
- Conocer y aceptar las condiciones de utilización de los certificados, en particular las contenidas en esta DPC y en la Política de Certificación, así como las modificaciones que se realicen sobre las mismas.
- Limitar y adecuar el uso del certificado a propósitos lícitos y acordes con los usos permitidos por la presente DPC
- Utilizar los certificados emitidos por PKIDEF sólo para aquellas transacciones, aplicaciones y ámbitos que estén autorizadas por la AGPMD.
- No utilizar un certificado digital que hubiera perdido su eficacia, por haber sido revocado o por haber expirado el periodo de validez del certificado.

9.6.4 Obligaciones de los Terceros Aceptantes

Es obligación de los terceros que acepten y confíen en los certificados emitidos por PKIDEF:

- Utilizar los certificados para los propósitos para los cuales fueron emitidos, tal y como se detalla en la información del certificado "KEY USAGE" y "EXTENDED KEY USAGE" (esto es, uso de clave y uso extendido de la clave) y en la presente DPC.
- Hacer uso del certificado única y exclusivamente en las aplicaciones autorizadas por el Ministerio de Defensa, previa autorización de la AGPMD.
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no ha caducado o ha sido revocado.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez, revocación o suspensión de los certificados en que confía y, en especial, de las EC que conforman la cadena de certificación.
- Hacer uso exclusivo de las Entidades de Validación y Sellado de Tiempo que presentan los servicios apropiados en las localizaciones descritas en la presente DPC.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

9.6.5 Obligaciones del repositorio

El Ministerio de Defensa mantiene publicadas las siguientes informaciones en DICODEF:

- Los certificados emitidos, incluidos los certificados de las Entidades de Certificación y otras Entidades de PKIDEF.
- Las listas de certificados revocados y otras informaciones del estado de revocación de los certificados.

Adicionalmente, el Ministerio de Defensa publica la presente Declaración de Prácticas de Certificación a través de un servicio de publicación web autorizado.

La presente DPC asume la integridad y veracidad de la información contenida en DICODEF y del resto de repositorios mencionados en ella. Es responsabilidad de los repositorios autorizados por esta DPC:

- Habilitar e implementar los procedimientos y mecanismos de seguridad que garanticen la disponibilidad, así como la veracidad e integridad de la información contenida en el mismo.
- Implantar mecanismos y procesos que garanticen la réplica de la información y recuperación de la misma.

9.7 *Renuncias de garantías*

PKIDEF puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, especialmente aquellas garantías de adaptación para un propósito particular del certificado.

9.8 *Limitaciones de responsabilidad*

El Ministerio de Defensa responderá por los daños y perjuicios que cause a cualquier persona, en el ejercicio de su actividad como Prestador de Servicios de Certificación, cuando se incumplan las obligaciones que le impone la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, o se actúe con negligencia.

El Ministerio de Defensa asume toda la responsabilidad frente a terceros por la actuación de las personas que realicen las funciones necesarias para la prestación del servicio de certificación.

El Ministerio de Defensa no asume ninguna responsabilidad en caso de pérdida o perjuicio:

- Ocasionado por el uso indebido o fraudulento de los certificados o CRL emitidos por PKIDEF.
- Ocasionado al firmante o terceros de buena fe si el destinatario de los documentos firmados electrónicamente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la CRL, o cuando no verifique la firma electrónica.

9.9 *Indemnizaciones*

No estipulado.

9.10 *Plazo y Finalización*

No estipulado.

9.11 *Notificaciones*

Toda notificación, demanda, solicitud o cualquier otra comunicación requerida bajo las prácticas descritas en esta DPC se realizará mediante conducto reglamentario, documento o mensaje electrónico firmado digitalmente, o por escrito oficial mediante correo certificado dirigido a cualquiera de las direcciones contenidas en la *sección 1.5.* Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

9.12 *Modificaciones*

Esta DPC entra en vigor desde el momento de su aprobación por la AGPMD y su publicación en los repositorios de PKIDEF. Esta DPC estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la EC, ocasión en que obligatoriamente se emitirá una nueva versión.

9.12.1 Procedimientos de especificación de cambios

Si se determinara que alguna sección o parte de esta DPC es incorrecta o no válida, el resto del documento permanecerá efectivo hasta que ésta se actualice.

La AGPMD revisará la presente DPC al menos una vez al año. Errores, actualizaciones o mejoras sobre este documento, deberán comunicarse al contacto identificado en la *sección 1.5*. Toda comunicación deberá incluir una descripción del cambio, su justificación y la información de la persona que solicita la modificación.

Todos los cambios aprobados en esta DPC por la AGPMD, serán difundidos a todas las partes interesadas según lo especificado en la *sección 9.12.2*. La AGPMD aceptará como modificaciones o rechazará los cambios propuestos tras haber completado su revisión.

9.12.2 Procedimientos de Publicación y Notificación

La AGPMD publicará toda la información relativa a la PKI del Ministerio de Defensa que considere oportuna (incluyendo la presente DPC), en un repositorio accesible a todos los usuarios de la PKIDEF.

La presente DPC actualizada y cuanta información se considere de interés se publicará en ***http://pki.mdef.es/cps/cps.htm***.

9.12.3 Procedimientos de Aprobación de la DPC

La presente DPC ha sido aprobada por la AGPMD, previa comprobación que el presente documento cumple con lo estipulado en la Política de Certificación del Ministerio de Defensa. Así mismo verifica que la EC-WPG cumple con los requerimientos expresados en la presente DPC para su puesta en operación.

9.13 *Resolución de conflictos*

Todas reclamaciones y disputas entre usuarios y PKIDEF deberán ser comunicadas por la parte en disputa a la AGPMD, para que resuelva la misma.

La AGPMD deberá resolver cualquier disputa que se derive sobre la interpretación o aplicabilidad de la presente DPC a la Política de Certificación.

Adicionalmente, el Ministerio de Defensa podrá establecer, a través de los instrumentos jurídicos mediante los que se articule su relación con subscriptores y verificadores, los procedimientos de mediación, arbitraje y resolución de conflictos que se consideren oportunos, todo ello sin perjuicio de la legislación de procedimiento administrativo.

9.14 *Legislación aplicable*

Las operaciones y funcionamiento de PKIDEF, así como la presente DPC, estarán sujetas a la legislación española. Explícitamente se asumen como de aplicación las siguientes normas:

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- La Orden de 21 de febrero de 2000 por la que se aprueba el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de forma electrónica.
- La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

9.15 *Conformidad con la Ley aplicable*

La AGPMD declara que la presente DPC cumple con las prescripciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

9.16 *Cláusulas Diversas*

No estipulado.

9.17 *Otras Cláusulas*

No estipulado.

Anexo 1 REFERENCIAS

RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. http://www.ietf.org/rfc/rfc3647.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. http://www.ietf.org/rfc/rfc5280.txt
X.501	ITU-T Recommendation X.501: Information Technology - Open Systems Interconnection - The Directory: Models.
X.509	ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework.
ETSI TS 102 042[9]	Policy requirements for certification authorities issuing public key certificates.
ETSI TS 101 456	Policy requirements for certification authorities issuing qualified certificates.
ETSI TS 102 280	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.
RFC 3739	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile. http://www.ietf.org/rfc/rfc3739.txt
ETSI TS 101 862	Qualified Certificate Profile.
RFC 2560	X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol (OCSP). http://www.ietf.org/rfc/rfc2560.txt
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). http://www.ietf.org/rfc/rfc3161.txt
ETSI TS 101 861	Time stamping profile.
RFC 3628	Policy Requirements for Time-Stamping Authorities (TSAs). http://www.ietf.org/rfc/rfc3628.txt
ETSI TS 102 023	Policy Requirements for Time Stamping Authorities Certificates for Electronic Signatures.

[9] Los estándares de ETSI relativos a firma electrónica pueden encontrarse en http://www.etsi.org/WebSite/Technologies/ElectronicSignature.aspx.

RFC 2251	Lightweight Directory Access Protocol (v3). http://www.faqs.org/rfcs/rfc2251.html
ETSI TS 101 733	CMS Advanced Electronic Signatures (CAdES).
ETSI TS 101 734	Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES).
ETSI TS 101 903	XML Advanced Electronic Signatures (XAdES).
ETSI TS 101 904	Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES).
ETSI TS 102 778	PDF Advanced Electronic Signature Profiles (PAdES).
CEN / ISSS: CWA 14167	CWA 14167-1 Security Requirements for Trustworthy Systems Managing. CWA 14167-2 Cryptographic module for CSP signing operations with backup. CWA 14167-3 Cryptographic module for CSP key generation services. CWA 14167-4 Cryptographic module for CSP signing operations.
CEN / ISSS: CWA 14169	Secure signature-creation devices “EAL 4+”.
CEN / ISSS: CWA 14172	EESSI Conformity Assessment Guidance.

Anexo 2 PERFILES DE CERTIFICADOS EMITIDOS POR LA EC-WPG

Anexo 2.1 CERTIFICADOS DE EMPLEADO PÚBLICO

2.1.1 Autenticación

Nombre del Perfil:	Certificado de Autenticación de Empleado Público de Nivel Alto
OID (Object Identifier):	2.16.724.1.1.1.1.3.11
Soporte:	TEMD
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Empleados públicos (personal civil y militar) de las diferentes unidades, centros y organismos (incluyendo organismos autónomos y públicos) del Ministerio de Defensa.
Registro:	Presencial. Se permiten hasta 2 renovaciones electrónicas remotas.
Usos Permitidos:	Identificación ante servicios, sistemas y aplicaciones informáticas pertenecientes al Ministerio de Defensa, a alguno de sus organismos vinculados o a Administraciones Públicas Locales, Autonómicas, Estatales, Internacionales o Corporativas. Identificación del personal al servicio de las Administraciones Públicas según la Ley 11/2007.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI según lo indicado en la Ley 11/2007.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		

Campo	Criticidad	Valor/Contenido
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Organizational Unit (OU)		OU = certificado electrónico de empleado público
1.6.5. Serial Number		SerialNumber = 00000000G
1.6.6. Common Name (CN)		JUAN ANTONIO DE LA CAMARA ESPAÑOL | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature
2.4. Extended Key Usage	NO	smartCardLogon, emailProtection, clientAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.11
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de autenticacion de empleado publico, nivel Alto, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***

Campo	Criticidad	Valor/Observaciones
2.6.3. QcSSCD		***OID 0.4.0.1862.1.4***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.7.2. User Principal Name (UPN)		UPN = juandelaespa12@mdef.es ***OID 1.3.6.1.4.1.311.20.2.3***
2.7.3. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***
2.7.3.1. Tipo de certificado		Tipo= "certificado electrónico de empleado público" ***OID 2.16.724.1.3.5.3.1.1***
2.7.3.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.3.1.2***
2.7.3.3. NIF entidad suscriptora		NIF = "S2800231I" ***OID 2.16.724.1.3.5.3.1.3***
2.7.3.4. DNI/NIE del responsable		DNI = 00000000G ***OID 2.16.724.1.3.5.3.1.4***
2.7.3.5. Nombre de pila		N = "JUAN ANTONIO" ***OID 2.16.724.1.3.5.3.1.6***
2.7.3.6. Primer apellido		SN1 = "DE LA CAMARA" ***OID 2.16.724.1.3.5.3.1.7***
2.7.3.7. Segundo apellido		SN2 = "ESPAÑOL" ***OID 2.16.724.1.3.5.3.1.8***
2.7.3.8. Correo electrónico		"juanantonio.delacamara.espanol@mde.es" ***OID 2.16.724.1.3.5.3.1.9***
2.8. Issuer Alternative Name	NO	
2.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.9. basicConstraints	SI	
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-

Campo	Criticidad	Valor/Observaciones
		WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method= On-line Certificate Status Protocol
2.11.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 12: Certificado de Autenticación de Empleado Público de Nivel Alto

2.1.2 Firma

Nombre del Perfil:	Certificado de Firma de Empleado Público de Nivel Alto
OID (Object Identifier):	2.16.724.1.1.1.1.3.12
Soporte:	TEMD
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Empleados públicos (personal civil y militar) de las diferentes unidades, centros y organismos (incluyendo organismos autónomos y públicos) del Ministerio de Defensa.
Registro:	Presencial. Se permiten hasta 2 renovaciones electrónicas remotas.
Usos Permitidos:	Firma electrónica avanzada (según Ley 59/2003) de correo electrónico o cualquier otra información o documento en el ejercicio de sus funciones. Permite dotar de evidencias criptográficas a aquellas acciones que exijan las características de integridad y de no repudio. Firma electrónica del personal al servicio de las Administraciones Públicas según la Ley 11/2007.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI según lo indicado en la Ley 11/2007. FIRMA ELECTRÓNICA AVANZADA según lo indicado en la Ley 59/2003.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		

Campo	Criticidad	Valor/Contenido
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Organizational Unit (OU)		OU = certificado electrónico de empleado público
1.6.5. Serial Number		SerialNumber = 00000000G
1.6.6. Common Name (CN)		JUAN ANTONIO DE LA CAMARA ESPAÑOL | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	nonRepudation
2.4. Extended Key Usage	NO	***No utilizado***
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.12

Campo	Criticidad	Valor/Observaciones
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de firma electronica de empleado publico, nivel Alto, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
2.6.3. QcSSCD		***OID 0.4.0.1862.1.4***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.7.2. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***
2.7.2.1. Tipo de certificado		Tipo= "certificado electrónico de empleado público" ***OID 2.16.724.1.3.5.3.1.1***
2.7.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.3.1.2***
2.7.2.3. NIF entidad suscriptora		NIF = "S2800231I" ***OID 2.16.724.1.3.5.3.1.3***
2.7.2.4. DNI/NIE del responsable		DNI = 00000000G ***OID 2.16.724.1.3.5.3.1.4***
2.7.2.5. Nombre de pila		N = "JUAN ANTONIO" ***OID 2.16.724.1.3.5.3.1.6***
2.7.2.6. Primer apellido		SN1 = "DE LA CAMARA" ***OID 2.16.724.1.3.5.3.1.7***
2.7.2.7. Segundo apellido		SN2 = "ESPAÑOL" ***OID 2.16.724.1.3.5.3.1.8***
2.7.2.8. Correo electrónico		"juanantonio.delacamara.espanol@mde.es" ***OID 2.16.724.1.3.5.3.1.9***
2.8. Issuer Alternative Name	NO	
2.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es

Campo	Criticidad	Valor/Observaciones
2.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.9. basicConstraints	SI	
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method= On-line Certificate Status Protocol
2.11.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 13: Certificado de Firma de Empleado Público de Nivel Alto

2.1.3 Cifrado

Nombre del Perfil:	Certificado de Cifrado de Empleado Público de Nivel Alto
OID (Object Identifier):	2.16.724.1.1.1.1.3.13
Soporte:	TEMD
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Empleados públicos (personal civil y militar) de las diferentes unidades, centros y organismos (incluyendo organismos autónomos y públicos) del Ministerio de Defensa.
Registro:	Presencial. Se permiten hasta 2 renovaciones electrónicas remotas.
Usos Permitidos:	Cifrado de correos electrónicos, mensajes, ficheros, transacciones informáticas u otra información a los que se quiera dotar de confidencialidad en el ejercicio de sus funciones. *Dado el limitado periodo de vida de los certificados, su uso es permitido únicamente para el transporte temporal de información sensible, prohibiéndose su utilización para custodiar y almacenar de forma permanente cualquier tipo de información.* Mecanismo de cifrado del personal al servicio de las Administraciones

	Públicas según la Ley 11/2007.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	SI
Certificado Reconocido	SI según lo indicado en la Ley 11/2007.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Organizational Unit (OU)		OU = certificado electrónico de empleado público
1.6.5. Serial Number		SerialNumber = 00000000G
1.6.6. Common Name (CN)		JUAN ANTONIO DE LA CAMARA ESPAÑOL | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***

Campo	Criticidad	Valor/Observaciones
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	keyEncipherment, dataEncipherment
2.4. Extended Key Usage	NO	emailProtection, clientAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.13
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de cifrado de empleado publico, nivel Alto, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
2.6.3. QcSSCD		***OID 0.4.0.1862.1.4***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.7.2. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***
2.7.2.1. Tipo de certificado		Tipo= "certificado electrónico de empleado público" ***OID 2.16.724.1.3.5.3.1.1***
2.7.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.3.1.2***
2.7.2.3. NIF entidad suscriptora		NIF = "S2800231I" ***OID 2.16.724.1.3.5.3.1.3***
2.7.2.4. DNI/NIE del responsable		DNI = 00000000G ***OID 2.16.724.1.3.5.3.1.4***
2.7.2.5. Nombre de pila		N = "JUAN ANTONIO" ***OID 2.16.724.1.3.5.3.1.6***
2.7.2.6. Primer apellido		SN1 = "DE LA CAMARA" ***OID 2.16.724.1.3.5.3.1.7***

Campo	Criticidad	Valor/Observaciones
2.7.2.7. Segundo apellido		SN2 = "ESPAÑOL" ***OID 2.16.724.1.3.5.3.1.8***
2.7.2.8. Correo electrónico		"juanantonio.delacamara.espanol@mde.es" ***OID 2.16.724.1.3.5.3.1.9***
2.8. Issuer Alternative Name	NO	
2.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.9. basicConstraints	SI	
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method= On-line Certificate Status Protocol
2.11.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 14: Certificado de Cifrado de Empleado Público de Nivel Alto

Anexo 2.2 CERTIFICADOS DE PERSONA FÍSICA

2.2.1 Autenticación

Nombre del Perfil:	Certificado de Autenticación de Persona Física en TEMD
OID (Object Identifier):	2.16.724.1.1.1.1.3.1
Soporte:	TEMD
Clave:	RSA 2048 bits

Periodo de Validez	24 meses
Suscriptores:	Personal civil externo que trabaja en el Ministerio de Defensa, bajo autorización de la AGPMD. Personal civil o militar externo cuyas actividades puedan tener especial relevancia para el Ministerio de Defensa, bajo autorización de la AGPMD.
Registro:	Presencial. Se permiten hasta 2 renovaciones electrónicas remotas.
Usos Permitidos:	Identificación ante servicios, sistemas y aplicaciones informáticas pertenecientes al Ministerio de Defensa, a alguno de sus organismos vinculados o a Administraciones Públicas Locales, Autonómicas, Estatales, Internacionales o Corporativas.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Common Name (CN)		JUAN ANTONIO DE LA CAMARA ESPAÑOL | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature
2.4. Extended Key Usage	NO	smartCardLogon, emailProtection, clientAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.1
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.6. Subject Alternate Names	NO	
2.6.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.6.2. User Principal Name (UPN)		UPN = juandelaespa12@mdef.es ***OID 1.3.6.1.4.1.311.20.2.3***
2.7. Issuer Alternative Name	NO	
2.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.8. basicConstraints	SI	
2.8.1. cA		FALSO
2.8.2. pathLenConstraint		***No utilizado***
2.9. cRLDistributionPoint	NO	
2.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method= On-line Certificate Status Protocol

Campo	Criticidad	Valor/Observaciones
2.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 15: Certificado de Autenticación de Persona Física en TEMD

2.2.2 Firma

Nombre del Perfil:	Certificado de Firma de Persona Física en TEMD
OID (Object Identifier):	2.16.724.1.1.1.1.3.2
Soporte:	TEMD
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Personal civil externo que trabaja en el Ministerio de Defensa, bajo autorización de la AGPMD. Personal civil o militar externo cuyas actividades puedan tener especial relevancia para el Ministerio de Defensa, bajo autorización de la AGPMD.
Registro:	Presencial. Se permiten hasta 2 renovaciones electrónicas remotas.
Usos Permitidos:	Firma electrónica avanzada (según Ley 59/2003) de correo electrónico o cualquier otra información o documento en el ejercicio de sus funciones. Permite dotar de evidencias criptográficas a aquellas acciones que exijan las características de integridad y de no repudio.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI. FIRMA ELECTRÓNICA AVANZADA según lo indicado en la Ley 59/2003.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		

Campo	Criticidad	Valor/Contenido
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Common Name (CN)		JUAN ANTONIO DE LA CAMARA ESPAÑOL | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	nonRepudation
2.4. Extended Key Usage	NO	***No utilizado***
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.2
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= " Certificado reconocido de firma electronica para persona fisica expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
2.6.3. QcSSCD		***OID 0.4.0.1862.1.4***

Campo	Criticidad	Valor/Observaciones
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.8. Issuer Alternative Name	NO	
2.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.9. basicConstraints	SI	
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method= On-line Certificate Status Protocol
2.11.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 16: Certificado de Firma de Persona Física en TEMD

2.2.3 Cifrado

Nombre del Perfil:	Certificado de Cifrado de Persona Física en TEMD
OID (Object Identifier):	2.16.724.1.1.1.1.3.3
Soporte:	TEMD
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Personal civil externo que trabaja en el Ministerio de Defensa, bajo autorización de la AGPMD. Personal civil o militar externo cuyas actividades puedan tener especial relevancia para el Ministerio de Defensa, bajo autorización de la AGPMD.

Registro:	Presencial. Se permiten hasta 2 renovaciones electrónicas remotas.
Usos Permitidos:	Cifrado de correos electrónicos, mensajes, ficheros, transacciones informáticas u otra información a los que se quiera dotar de confidencialidad en el ejercicio de sus funciones. *Dado el limitado periodo de vida de los certificados, su uso es permitido únicamente para el transporte temporal de información sensible, prohibiéndose su utilización para custodiar y almacenar de forma permanente cualquier tipo de información.*
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	SI
Certificado Reconocido	NO.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Common Name (CN)		JUAN ANTONIO DE LA CAMARA ESPAÑOL | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-

Campo	Criticidad	Valor/Observaciones
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	keyEncipherment, dataEncipherment
2.4. Extended Key Usage	NO	emailProtection, clientAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.3
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.6. Subject Alternate Names	NO	
2.6.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.7. Issuer Alternative Name	NO	
2.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.8. basicConstraints	SI	
2.8.1. cA		FALSO
2.8.2. pathLenConstraint		***No utilizado***
2.9. cRLDistributionPoint	NO	
2.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method= On-line Certificate Status Protocol
2.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 17: Certificado de Cifrado de Persona Física en TEMD

Anexo 2.3 CERTIFICADOS DE SEDE ELECTRÓNICA

2.3.1 Nivel Alto

Nombre del Perfil:	Certificado de Sede Electrónica de Nivel Alto
OID (Object Identifier):	2.16.724.1.1.1.1.3.10
Soporte:	HSM
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias en la relación con el ciudadano.
Registro:	Solicitud electrónica remota a través del titular de la Sede o un representante, que actúa como Agente de la PKI.
Usos Permitidos:	Dotar a las sedes electrónicas de capacidades SSL/TLS. Permite la identificación inequívoca, así como el establecimiento de comunicaciones seguras (incluyendo el cifrado del canal de los datos transmitidos) de las sedes electrónicas con los servicios y aplicaciones informáticas, según la Ley 11/2007.
Publicación:	SubRama sede electrónica, Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI según lo indicado en la Ley 11/2007.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF

Campo	Criticidad	Valor/Contenido
1.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
1.6.4. Organizational Unit (OU)		OU= sede electrónica
1.6.5. Organizational Unit (OU)		OU= SEDE ELECTRONICA DEL MINISTERIO DE DEFENSA
1.6.6. Serial Number		SerialNumber = Sxxxxxxxx ***NIF del Departamento del Ministerio de Defensa responsable de la SEDE.***
1.6.7. Common Name (CN)		CN= sede.defensa.gob.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature, keyEncipherment
2.4. Extended Key Usage	NO	serverAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.10
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de sede electronica, nivel Alto, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Subject Alternate Names	NO	
2.6.1. rfc822Name		rfc822Name= sede@oc.mde.es
2.6.2. dnsName		dnsName= sede.defensa.gob.es
2.6.3. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***

Campo	Criticidad	Valor/Observaciones
2.6.3.1. Tipo de certificado		Tipo= "sede electrónica" ***OID 2.16.724.1.3.5.1.1.1***
2.6.3.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.1.1.2***
2.6.3.3. NIF entidad suscriptora		NIF = "Sxxxxxxxx" ***OID 2.16.724.1.3.5.1.1.3***
2.6.3.4. Nombre descriptivo de la Sede		Nombre sede = "SEDE ELECTRONICA DEL MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.1.1.4***
2.6.3.5. Denominación de nombre de dominio IP		Nombre Dominio IP = "sede.defensa.gob.es" ***OID 2.16.724.1.3.5.1.1.5***
2.7. Issuer Alternative Name	NO	
2.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.8. basicConstraints	SI	
2.8.1. cA		FALSO
2.8.2. pathLenConstraint		***No utilizado***
2.9. cRLDistributionPoint	NO	
2.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method= On-line Certificate Status Protocol
2.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 18: Certificado de Sede Electrónica de Nivel Alto

2.3.2 Nivel Medio

Nombre del Perfil:	Certificado de Sede Electrónica de Nivel Medio
OID (Object Identifier):	2.16.724.1.1.1.1.2.10
Soporte:	Software
Clave:	RSA 1024 bits
Periodo de Validez	24 meses
Suscriptores:	Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias en la relación con el ciudadano.
Registro:	Solicitud electrónica remota a través del titular de la Sede o un representante, que actúa como Agente de la PKI.
Usos Permitidos:	Dotar a las sedes electrónicas de capacidades SSL/TLS. Permite la identificación inequívoca, así como el establecimiento de comunicaciones seguras (incluyendo el cifrado del canal de los datos transmitidos) de las sedes electrónicas con los servicios y aplicaciones informáticas, según la Ley 11/2007.
Publicación:	SubRama sede electrónica, Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI según lo indicado en la Ley 11/2007.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
1.6.4. Organizational Unit (OU)		OU= sede electrónica

Campo	Criticidad	Valor/Contenido
1.6.5. Organizational Unit (OU)		OU= SEDE ELECTRONICA DEL MINISTERIO DE DEFENSA
1.6.6. Serial Number		SerialNumber = Sxxxxxxxx ***NIF del Departamento del Ministerio de Defensa responsable de la SEDE.***
1.6.7. Common Name (CN)		CN= sede.defensa.gob.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de de al menos 1024 bits para un certificado de nivel medio.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature, keyEncipherment
2.4. Extended Key Usage	NO	serverAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.10
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de sede electronica, nivel Medio, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Subject Alternate Names	NO	
2.6.1. rfc822Name		rfc822Name= sede@oc.mde.es
2.6.2. dnsName		dnsName= sede.defensa.gob.es
2.6.3. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***
2.6.3.1. Tipo de certificado		Tipo= "sede electrónica" ***OID 2.16.724.1.3.5.1.2.1***

Campo	Criticidad	Valor/Observaciones
2.6.3.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.1.2.2***
2.6.3.3. NIF entidad suscriptora		NIF = "Sxxxxxxxx" ***OID 2.16.724.1.3.5.1.2.3***
2.6.3.4. Nombre descriptivo de la Sede		Nombre sede = "SEDE ELECTRONICA DEL MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.1.2.4***
2.6.3.5. Denominación de nombre de dominio IP		Nombre Dominio IP = "sede.defensa.gob.es" ***OID 2.16.724.1.3.5.1.2.5***
2.7. Issuer Alternative Name	NO	
2.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.8. basicConstraints	SI	
2.8.1. cA		FALSO
2.8.2. pathLenConstraint		***No utilizado***
2.9. cRLDistributionPoint	NO	
2.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method= On-line Certificate Status Protocol
2.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 19: Certificado de Sede Electrónica de Nivel Medio

Anexo 2.4 CERTIFICADOS DE SELLO ELECTRÓNICO

2.4.1 Nivel Alto

Nombre del Perfil:	Certificado de Sello Electrónico de Nivel Alto

OID (Object Identifier):	2.16.724.1.1.1.1.3.14
Soporte:	HSM
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias en la relación con el ciudadano.
Registro:	Solicitud electrónica remota a través del titular del Sello o un representante, que actúa como Agente de la PKI.
Usos Permitidos:	Puede utilizarse en actuaciones automatizadas para la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante y el cifrado de datos frente a servicios y aplicaciones informáticas. Sistema de firma electrónica para la actuación administrativa automatizada según la Ley 11/2007.
Publicación:	SubRama sello electrónico, Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI según lo indicado en la Ley 11/2007.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = GENERICAS
1.6.4. Organizational Unit (OU)		OU = sello electrónico
1.6.5. Serial Number		SerialNumber = Sxxxxxxxx

Campo	Criticidad	Valor/Contenido
		NIF del Departamento del Ministerio responsable del SELLO.
1.6.6. Common Name (CN)		CN= SELLO SISTEMA AUTOMATIZADO DEL MINISTERIO DE DEFENSA
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits por tratarse de un certificado de nivel alto.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
2.4. Extended Key Usage	NO	clientAuth, emailProtection
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.14
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de sello electronico, nivel Alto, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
2.6.3. QcSSCD		***OID 0.4.0.1862.1.4***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= sello@oc.mde.es
2.7.2. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***

Campo	Criticidad	Valor/Observaciones
2.7.2.1. Tipo de certificado		Tipo= "sello electrónico" ***OID 2.16.724.1.3.5.2.1.1***
2.7.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.2.1.2***
2.7.2.3. NIF entidad suscriptora		NIF = "Sxxxxxxxx" ***OID 2.16.724.1.3.5.2.1.3***
2.7.2.4. Denominación de sistema o componente		Denominación sistema = "SELLO SISTEMA AUTOMATIZADO DEL MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.2.1.5***
2.8. Issuer Alternative Name	NO	
2.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.9. basicConstraints	SI	
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method= On-line Certificate Status Protocol
2.11.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 20: Certificado de Sello Electrónico de Nivel Alto

2.4.2 Nivel Medio

Nombre del Perfil:	Certificado de Sello Electrónico de Nivel Medio
OID (Object Identifier):	2.16.724.1.1.1.1.2.14

Soporte:	Software
Clave:	RSA 1024 bits
Periodo de Validez	24 meses
Suscriptores:	Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias en la relación con el ciudadano.
Registro:	Solicitud electrónica remota a través del titular del Sello o un representante, que actúa como Agente de la PKI.
Usos Permitidos:	Puede utilizarse en actuaciones automatizadas para la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante y el cifrado de datos frente a servicios y aplicaciones informáticas. Sistema de firma electrónica para la actuación administrativa automatizada según la Ley 11/2007.
Publicación:	SubRama sello electrónico, Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	SI según lo indicado en la Ley 11/2007.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = GENERICAS
1.6.4. Organizational Unit (OU)		OU = sello electrónico
1.6.5. Serial Number		SerialNumber = Sxxxxxxxx ***NIF del Departamento del Ministerio responsable del SELLO.***

Campo	Criticidad	Valor/Contenido
1.6.6. Common Name (CN)		CN= SELLO SISTEMA AUTOMATIZADO DEL MINISTERIO DE DEFENSA
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de de al menos 1024 bits para un certificado de nivel medio.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
2.4. Extended Key Usage	NO	clientAuth, emailProtection
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.14
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.5.2.2. User Notice		Notice Text= "Certificado reconocido de sello electronico, nivel Medio, expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= sello@oc.mde.es
2.7.2. Directory Name		***Campos específicos definidos por la Administración para los certificados LAECSP.***
2.7.2.1. Tipo de certificado		Tipo= "sello electrónico" ***OID 2.16.724.1.3.5.2.2.1***

Campo	Criticidad	Valor/Observaciones
2.7.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.2.2.2***
2.7.2.3. NIF entidad suscriptora		NIF = "Sxxxxxxxx" ***OID 2.16.724.1.3.5.2.2.3***
2.7.2.4. Denominación de sistema o componente		Denominación sistema = "SELLO SISTEMA AUTOMATIZADO DEL MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.2.2.5***
2.8. Issuer Alternative Name	NO	
2.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
2.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.9. basicConstraints	SI	
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method= On-line Certificate Status Protocol
2.11.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 21: Certificado de Sello Electrónico de Nivel Medio

Anexo 2.5 CERTIFICADOS DE DISPOSITIVO

2.5.1 Servidor Seguro (SSL) / Dispositivo

Nombre del Perfil:	Certificado de Servidor Seguro o Dispositivo del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.5

Soporte:	Software
Clave:	RSA 1024 bits
Periodo de Validez	24 meses
Suscriptores:	Estaciones de trabajo, firewalls, routers, cifradores en línea, servidores (bases de datos, FTP o web) y otros componentes de la infraestructura del Ministerio de Defensa.
Registro:	Solicitud electrónica remota a través del responsable del servidor o dispositivo, que actúa como Agente de la PKI.
Usos Permitidos:	Permite la identificación segura de los servidores y dispositivos de la infraestructura del Ministerio de Defensa, así como el establecimiento de comunicaciones seguras (incluyendo el cifrado del canal de los datos transmitidos), dotándolos de capacidades SSL/TLS.
Publicación:	Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	NO

Campo	Criticidad	Valor/Contenido
3. X.509v1 Field		
3.1. Version		2
3.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
3.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
3.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
3.5. Validity		24 meses
3.5.1. Not Before		
3.5.2. Not After		
3.6. Subject		
3.6.1. Country (C)		C = ES
3.6.2. Organization (O)		O = MDEF
3.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
3.6.4. Common Name (CN)		CN = www.mde.es CN = router.mdef.es
3.7. Subject Public Key Info		RSAEncryption

Campo	Criticidad	Valor/Contenido
		OID 1.2.840.113549.1.1.1 ***Longitud de 1024 bits.***

Campo	Criticidad	Valor/Observaciones
4. X.509v3 Extensions		-
4.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
4.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
4.3. Key Usage	SI	digitalSignature, keyEncipherment
4.4. Extended Key Usage	NO	serverAuth
4.5. Certificate Policies	NO	
4.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.5
4.5.2. Policy Qualifier ID		
4.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
4.6. Subject Alternate Names	NO	
4.6.1. dnsName		dnsName= www.mde.es dnsName= router.mdef.es
4.7. Issuer Alternative Name	NO	
4.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
4.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
4.8. basicConstraints	SI	
4.8.1. cA		FALSO
4.8.2. pathLenConstraint		***No utilizado***
4.9. cRLDistributionPoint	NO	
4.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
4.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint

Campo	Criticidad	Valor/Observaciones
4.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
4.10. Authority Info Access	NO	
4.10.1. Access Method		Access Method= On-line Certificate Status Protocol
4.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 22: Certificado de Servidor Seguro (SSL) / Dispositivo

2.5.2 Controlador de Dominio

Nombre del Perfil:	Certificado de Controlador de Dominio del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.5
Soporte:	Software
Clave:	RSA 1024 bits
Periodo de Validez	24 meses
Suscriptores:	Controladores de dominio de la infraestructura de Directorio Activo de Windows del Ministerio de Defensa.
Registro:	Solicitud electrónica remota a través del responsable del controlador de dominio, que actúa como Agente de la PKI.
Usos Permitidos:	Permite la identificación del servidor como controlador de dominio la infraestructura de Directorio Activo de Windows del Ministerio de Defensa, garantizando la confianza de los controladores de dominio en los certificados de autenticación emitidos por EC-WPG y permitiendo el inicio de sesión de los usuarios con una TEMD válida en sistemas operativos Windows con dichos certificados.
Publicación:	Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***

Campo	Criticidad	Valor/Contenido
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
1.6.4. Common Name (CN)		CN = domaincontroller.mdef.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 1024 bits.***

Campo	Criticidad	Valor/Observaciones
2. X.509v3 Extensions		-
2.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
2.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
2.3. Key Usage	SI	digitalSignature, keyEncipherment
2.4. Extended Key Usage	NO	clientAuth, serverAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.5
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
2.6. Subject Alternate Names	NO	
2.6.1. dnsName		dnsName= domaincontroller.mdef.es
2.6.2. otherName		1.3.6.1.4.1.311.25.1 = 04 10 96 8e ea d7 ee ba bc 42 81 db 4f 92 f5 88 db 4a
2.7. Issuer Alternative Name	NO	
2.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es

Campo	Criticidad	Valor/Observaciones
2.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.8. basicConstraints	SI	
2.8.1. cA		FALSO
2.8.2. pathLenConstraint		***No utilizado***
2.9. cRLDistributionPoint	NO	
2.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method= On-line Certificate Status Protocol
2.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308
2.11. Certificate Template Name		DomainController

Ilustración 23: Certificado de Controlador de Dominio

Anexo 2.6 CERTIFICADOS DE SISTEMA O APLICACIÓN

2.6.1 Autenticación NO PERSONA

Nombre del Perfil:	Certificado de Autenticación NO PERSONA para sistemas y aplicaciones del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.9
Soporte:	Software
Clave:	RSA 1024 bits
Periodo de Validez	24 meses
Suscriptores:	Sistemas y aplicaciones del Ministerio de Defensa.
Registro:	Solicitud electrónica remota a través del responsable del sistema o aplicación, que actúa como Agente de la PKI.
Usos Permitidos:	Puede utilizarse como mecanismo de identificación de las aplicaciones y sistemas frente a la Plataforma de servicios de Seguridad del Ministerio de

	Defensa (PSSDEF). También puede ser usado para identificación de equipos en redes WIFI, usando EAP-TLS y Radius.
Publicación:	Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
1.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MDEF
1.6.3. Organizational Unit (OU)		OU = GENERICAS
1.6.4. Organizational Unit (OU)		OU = PSSDEF ***Opcional***
1.6.5. Common Name (CN)		CN = Sistema MDEF
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 1024 bits.***

Campo	Criticidad	Valor/Observaciones
3. X.509v3 Extensions		-
3.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***

Campo	Criticidad	Valor/Observaciones
3.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
3.3. Key Usage	SI	digitalSignature, keyEncipherment, keyAgreement
3.4. Extended Key Usage	NO	clientAuth
3.5. Certificate Policies	NO	
3.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.9
3.5.2. Policy Qualifier ID		
3.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
3.6. Subject Alternate Names	NO	
3.6.1. dnsName		dnsName= sistema.mdef.es ***Opcional para identificación en redes WIFI***
3.7. Issuer Alternative Name	NO	
3.7.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
3.7.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
3.8. basicConstraints	SI	
3.8.1. cA		FALSO
3.8.2. pathLenConstraint		***No utilizado***
3.9. cRLDistributionPoint	NO	
3.9.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
3.9.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
3.9.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
3.10. Authority Info Access	NO	
3.10.1. Access Method		Access Method= On-line Certificate Status Protocol
3.10.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 24: Certificado de Autenticación NO PERSONA

2.6.2 Firma NO PERSONA

Nombre del Perfil:	Certificado de Firma NO PERSONA para sistemas y aplicaciones del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.8
Soporte:	Software
Clave:	RSA 1024 bits
Periodo de Validez	24 meses
Suscriptores:	Sistemas y aplicaciones del Ministerio de Defensa.
Registro:	Solicitud electrónica remota a través del responsable del sistema o aplicación, que actúa como Agente de la PKI.
Usos Permitidos:	Puede utilizarse como mecanismo de identificación de las aplicaciones y para la firma electrónica y/o cifrado de datos por parte de éstas. También puede ser usado para la firma y cifrado de mensajería SOAP (WS-Security) en Servicios Web.
Publicación:	Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Reconocido	NO

Campo	Criticidad	Valor/Contenido
2. X.509v1 Field		
2.1. Version		2
2.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
2.3. Signature Algorithm		SHA-1WithRSAEncryption ***OID 1:2:840:113549:1:1:5***
2.4. Issuer Distinguished Name		CN = MINISDEF-EC-WPG, OU = PKI, O = MDEF, C = ES
2.5. Validity		24 meses
2.5.1. Not Before		
2.5.2. Not After		
2.6. Subject		
2.6.1. Country (C)		C = ES
2.6.2. Organization (O)		O = MDEF
2.6.3. Organizational Unit (OU)		OU = GENERICAS

Campo	Criticidad	Valor/Contenido
2.6.4. Organizational Unit (OU)		OU = PSSDEF ***Opcional***
2.6.5. Common Name (CN)		CN = Sistema MDEF
2.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 1024 bits.***

Campo	Criticidad	Valor/Observaciones
4. X.509v3 Extensions		-
4.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
4.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
4.3. Key Usage	SI	digitalSignature, keyEncipherment, dataEncipherment
4.4. Extended Key Usage	NO	clientAuth, emailProtection
4.5. Certificate Policies	NO	
4.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.8
4.5.2. Policy Qualifier ID		
4.5.2.1. CPS Pointer		http://pki.mdef.es/cps/cps.htm
4.6. Issuer Alternative Name	NO	
4.6.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
4.6.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
4.7. basicConstraints	SI	
4.7.1. cA		FALSO
4.7.2. pathLenConstraint		***No utilizado***
4.8. cRLDistributionPoint	NO	
4.8.1. distributionPoint		URL= ldap:///CN=MINISDEF-EC-WPG,CN=EC-WPG,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=et,DC=mde,DC=es?certificateRevocationList?base?objectclass=cRLDistributionPoint
4.8.2. distributionPoint		URL= ldap://ldap.mdef.es/cn=MINISDEF-CRL-EC-WPG,OU=PKI,O=MDEF,C=ES?certificateRevocationList?ba

Campo	Criticidad	Valor/Observaciones
		se?objectclass=cRLDistributionPoint
4.8.3. distributionPoint		URL= http://pki.mdef.es/crl/MINISDEF-CRL-EC-WPG.crl
4.9. Authority Info Access	NO	
4.9.1. Access Method		Access Method= On-line Certificate Status Protocol
4.9.2. Access Location		URL= http://ev01-wpg.mdef.es:9308

Ilustración 25: Certificado de Firma NO PERSONA

Anexo 3 CERTIFICADOS DE LAS ENTIDADES DE CERTIFICACIÓN DE PKIDEF

Anexo 3.1 EC RAÍZ

Campo	Contenido	Critica
1. Versión	V3	
2. Número de Serie	Número Entero	
3. Algoritmo de Firma	SHA-1WithRSAEncryption	
4. Emisor	CN=MINISDEF-EC-RAIZ, OU=PKI, O=MDEF, C=ES	
5. Validez	36 años	
6. Titular	CN=MINISDEF-EC-RAIZ, OU=PKI, O=MDEF, C=ES	
7. Información Clave Pública Titular	Algoritmo: RSA Encryption Longitud clave: 4096 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	No utilizado	
2. subjectUniqueIdentifier	No utilizado	
Extensiones de X509v3		
1. Identificador Clave del Titular	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Identificador Clave de la Entidad	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.	NO
3. Uso de Clave		SI
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	1	
CRL Signature	1	
4.Uso Extendido de Clave	No utilizado	NO
5. Período de Uso de la Clave Privada	No utilizado	
6. Políticas de Certificados		NO
Identificador Política	2.5.29.32.0 (anyPolicy)	
URL CPS	http://pki.mdef.es/cps/cps.htm	
7. Mapeos de Políticas	No utilizado	NO
8. Nombres Alternativos del Titular	directoryName= CN=Entidad de Certificacion Raiz, OU=Ministerio de Defensa de España, OU=PKI, O=MDEF, C=ES	NO
9. Nombres Alternativos del Emisor	No utilizado	
10. Atributos de Directorio del Titular	No utilizado	
11. Restricciones básicas		SI
CA	Sí	
Restricción Longitud Ruta Certificación	Ninguno	
12. Punto Distribución de CRLs	No utilizado	NO

Campo	Contenido	Critica
13. Acceso a Información de la Entidad	No utilizado	
14. Extensiones Netscape	No utilizado	NO
15. Restricciones de Nombre	No utilizado	
16. Restricciones de Política	No utilizado	

Ilustración 26: Certificado EC-RAIZ

Anexo 3.2 EC SUBORDINADA

Campo	Contenido	Critica
1. Versión	V3	
2. Número de Serie	Número Entero	
3. Algoritmo de Firma	SHA-1WithRSAEncryption	
4. Emisor	CN=MINISDEF-EC-RAIZ, OU=PKI, O=MDEF, C=ES	
5. Validez	11 años	
6. Titular	CN=MINISDEF-EC-WPG, OU=PKI O=MDEF, C=ES	
7. Información Clave Pública Titular	Algoritmo: RSA Encryption Longitud clave: 2048 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	No utilizado	
2. subjectUniqueIdentifier	No utilizado	
Extensiones de X509v3		
1. Identificador Clave del Titular	Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.	NO
2. Identificador Clave de la Entidad	Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.	NO
3. Uso de Clave		SI
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	1	
CRL Signature	1	
4.Uso Extendido de Clave	No utilizado	NO
5. Período de Uso de la Clave Privada	No utilizado	
6. Políticas de Certificados		NO
Identificador Política	2.16.724.1.1.1.1.1 2.16.724.1.1.1.1.2 2.16.724.1.1.1.1.3 2.16.724.1.1.1.1.4	
URL CPS	http://pki.mdef.es/cps/cps.htm	
7. Mapeos de Políticas	No utilizado	NO
8. Nombres Alternativos del Titular	directoryName= CN=Entidad de Certificacion Subordinada WPG, OU=Ministerio de Defensa de España, OU=PKI,	NO

Campo	Contenido	Critica
	O=MDEF, C=ES	
9. Nombres Alternativos del Emisor	No utilizado	
10. Atributos de Directorio del Titular	No utilizado	
11. Restricciones básicas		SI
CA	Sí	
Restricción Longitud Ruta Certificación	Ninguno	
12. Punto Distribución de CRLs	ldap:///CN=MINISDEF-EC-RAIZ,CN=EC-RAIZ,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=ET,DC=MDE,DC=ES?certificateRevocationList?base?objectclass=cRLDistributionpoint ldap:///ldap.mdef.es/cn=MINISDEF-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base? objectclass=cRLDistributionpoint http://pki.mdef.es/crl/MINISDEF-CRL-EC-RAIZ.crl	NO
13. Acceso a Información de la Entidad	No utilizado	
14. Extensiones Netscape	No utilizado	NO
15. Restricciones de Nombre	No utilizado	
16. Restricciones de Política	No utilizado	

Ilustración 27: Certificado EC-WPG

Anexo 4 APLICACIONES HABILITADAS POR LA AGPMD

La presente DPC entiende por aplicación habilitada cualquiera que teniendo necesidad de uso de alguno de los servicios de seguridad ofrecidos por PKIDEF (certificados digitales, sellado de tiempo y validación de certificados) haya sido autorizada para tal fin por la AGPMD, una vez los responsables de la aplicación y la Subunidad de PKI hayan asegurado la viabilidad tecnológica en el uso de los certificados.

Actualmente PKIDEF emite certificados electrónicos de:

- Persona Física: autenticación, firma reconocida, cifrado.
- Empleado Público según la Ley 11/2007: autenticación, firma reconocida, cifrado.
- Sede Electrónica y Sello Electrónico según la Ley 11/2007.
- Dispositivos: servidores seguros (SSL), routers, controladores
- Sistemas y aplicaciones: Firma (no persona) y autenticación (no persona)
- Firma de Código

Como norma general, **todas las aplicaciones y sistemas del Ministerio de Defensa (tanto de ámbito privado como público)[10] están habilitadas** para usar todos los certificados cuya tipología está presentada en la presente DPC, así como los servicios de sellado de tiempo y validación de certificados.

La autorización se considerará definitiva tras la entrega del certificado correspondiente al sistema o aplicación (previa solicitud a través de SCANS), o su inclusión en la plataforma PSSDEF (través del procedimiento de solicitud de alta correspondiente en SCANS).

La AGPMD podrá denegar la solicitud del servicio cuando considere que se pone en riesgo la prestación del servicio de PKIDEF o la seguridad del mismo, bien porque se vaya en contra de las directrices expresadas en la presente DPC o en la Política de Seguridad de la Información del Ministerio de Defensa.

El uso de certificados emitidos por el Ministerio de Defensa en aplicaciones de terceros (otras Administraciones, organismos o empresas externas) **requerirá la aprobación de la AGPMD**, previa petición oficial de los interesados, y tras alcanzarse los correspondientes acuerdos de colaboración con las organizaciones externas involucradas.

10 Aplicaciones de ámbito privado: aquellas de tipo exclusivamente interno a las que sólo acceden usuarios internos u otros sistemas del Ministerio de Defensa. Aplicaciones de ámbito público: aquellas a las que accedan usuarios externos, o que se interrelacionen con sistemas de otras Administraciones, organismos o empresas externas.

Anexo 5 PRESTACIÓN DE LOS SERVICIOS DE VALIDACIÓN A ENTIDADES EXTERNAS

La presente DPC permite la prestación del servicio de validación a aquellas entidades externas al Ministerio de Defensa, una vez hayan sido estas aprobadas por la AGPMD.

Estas entidades autorizadas serán notificadas al Responsable de la Subunidad de PKI para que este habilite y garantice la prestación del servicio en las condiciones de uso y seguridad recogidas en la presente DPC. Dicho responsable está habilitado para la denegación del servicio cuando considere que se pone en riesgo la operativa de seguridad o prestación del servicio dentro del CCEA. Este tipo de incidencias deben ser resueltas en el ámbito de la AGPMD y la Subunidad de PKI del CCEA.

La inclusión de nuevas entidades no supone causa de modificación de la presente DPC estando dicha circunstancia sujeta en última instancia a la AGPMD.

Anexo 6 PERFILES DE CONFIANZA Y CRITERIOS DE SEGREGACIÓN DE PERFILES

La segregación de los perfiles de gestión, dada la especial naturaleza de los servicios de seguridad que se ofrecen, aplica de manera taxativa a los perfiles de los operadores de los sistemas de PKIDEF y los Operadores de los HSM. Por razones de operativa se permite el solapamiento en los distintos perfiles operacionales, siendo disjuntos dentro de los distintos roles que aplican a cada uno.

Perfil	***Operativa***
Perfiles Operativos de la Infraestructura de Clave Pública[11].	
Oficial de Seguridad	Existen en todo momento al menos dos oficiales de seguridad distintos en las instalaciones del CCEA.
Oficial de Registro	Existen en todo momento al menos dos oficiales de registro distintos en las instalaciones del CCEA
Oficial de Administración	Existen en todo momento al menos dos oficiales de administración distintos en las instalaciones del CCEA
Auditor Sistema	Existen en todo momento al menos dos auditores de administración distintos en las instalaciones del CCEA
Oficial de Revocación Masiva	Existen en todo momento al menos un oficial de revocación masiva en la Subunidad de PKI del CCEA y un oficial de revocación masiva en la AGPMD.
Oficial de Revocación de Operador de ERL	Existen en todo momento al menos un oficial de revocación masiva en la Subunidad de PKI del CCEA y un oficial de revocación masiva en la AGPMD.
Perfiles Operativos de la Gestión de la Subunidad de PKI del CCEA[12]	
Responsable de la Subunidad de PKI[13].	Existe en todo momento un Responsable de la Subunidad de PKI en las instalaciones del CCEA.
Llavero	Existe en todo momento un Llavero en las instalaciones del Departamento de PKI.
Perfiles Operativos de la Gestión de los Módulos HSM de la Infraestructura de Clave Pública[14].	

11 No está permitido el solapamiento de los perfiles presentados en ningún caso.

12 Se permite el solapamiento de dichos perfiles con los perfiles de Operativa de PKI si bien entre ellos son mutuamente exclusivos.

13 El Responsable del Departamento ostenta de manera personal los perfiles de Revocación Masiva y Revocación de Operador de ERL para el caso de necesidad de urgencia de dicha operativa desde las instalaciones del CCEA.

Oficial Seguridad Primero HSM EC Raíz	Existen en todo momento al menos un Oficial de Seguridad Primero en las instalaciones del CCEA
Oficial Seguridad Segundo HSM EC Raíz.	Existen en todo momento al menos un Oficial de Seguridad Segundo en las instalaciones del CCEA
Oficial OCS HSM EC Subordinada	Existen en todo momento al menos un Oficial OCS en las instalaciones del CCEA
Oficial ACS HSM EC Subordinada	Existen en todo momento al menos un Oficial ACS en las instalaciones del CCEA

Ilustración 28: Perfiles de gestión del Ministerio de Defensa

Por ello, el conjunto mínimo de operadores que deben estar de forma presencial en la Subunidad de PKI del CCEA son **8**, debiendo estar presentes al menos **2** personas en las facilidades de la AGPMD.

14 No se permite en ningún caso el solapamiento de los oficiales de seguridad de los módulos independientemente de la jerarquía de los mismos. Se permite sin embargo el solapamiento de dichos perfiles con los operativos de PKI y Operativos del Departamento.

Anexo 7 PLANTILLAS DE USO EN LA ENTIDAD DE REGISTRO LOCAL

Se presentan a continuación las plantillas que se firman por los solicitantes en los puestos de Entidad de Registro Local.

PKI del Ministerio de Defensa

SOLICITUD DE EMISIÓN DE NUEVO CERTIFICADO

ENTIDAD EMISORA:

FECHA:	ERL EMISORA:
$$dd/$$mm/$$aaaa	$$raOperator

SUBSCRIPTOR O AGENTE:

E-MAIL:	DNI / PASAPORTE /TIM:
$$email	$$dni

NOMBRE:

$$givenName

APELLIDOS:

$$surname1 $$surname2

TIPOLOGÍA DE LOS CERTIFICADOS A EMITIR:

TIPOLOGIA	**X**	Autenticación y Correo Electrónico

	X	Firma Electrónica
	X	Cifrado Digital
		Servidor / Dispositivo / Otros
NIVEL	**$$ sw**	Nivel 2 (Software)
	$$ hw	Nivel 2 HW (Tarjeta Electrónica)

SERVIDOR / DISPOSITIVO / OTROS:

IDENTIFICADOR: LOCALIZACIÓN:

FUNCIÓN:

Firma de Servidor	*Servidor Seguro*	*Dispositivo HW*	*Controlador de Dominio*	*Firma de Código*

El Operador de la ERL,

Fecha: $$dd / $$mm / $$aaaa

El operador de la ERL certifica que toda la información presentada es correcta y que cumple con las condiciones expresadas en la Política de Certificación de la PKI del Ministerio de Defensa.

El Solicitante,

Fecha: $$dd / $$mm / $$aaaa

El solicitante declara que los datos expuestos son correctos.

PKI del Ministerio de Defensa

SOLICITUD DE RENOVACIÓN DE UN CERTIFICADO

ENTIDAD EMISORA:

FECHA:	ERL EMISORA:
$$dd/$$mm/$$aaaa	$$raOperator

SUBSCRIPTOR O AGENTE:

E-MAIL:	DNI / PASAPORTE /TIM:
$$email	$$dni

NOMBRE:

$$givenName

APELLIDOS:

$$surname1 $$surname2

TIPOLOGÍA DE LOS CERTIFICADOS A RENOVAR:

TIPOLOGIA	X	Autenticación y Correo Electrónico
	X	Firma Electrónica

	X	Cifrado Digital
		Servidor / Dispositivo / Otros
NIVEL	**$$ sw**	Nivel 2 (Software)
	$$ hw	Nivel 2 HW (Tarjeta Electrónica)

AVISO DE RENOVACIÓN:

CÓDIGO DE REFERENCIA:

SERVIDOR / DISPOSITIVO / OTROS:

IDENTIFICADOR: LOCALIZACIÓN:

FUNCIÓN:

Firma de Servidor	*Servidor Seguro*	*Dispositivo HW*	*Controlador de Dominio*	*Firma de Código*

El Operador de la ERL, El Solicitante,

Fecha: $$dd / $$mm / $$aaaa

El operador de la ERL certifica que toda la información presentada es correcta y que cumple con las condiciones expresadas en la Política de Certificación de la PKI del Ministerio de Defensa.

Fecha: $$dd / $$mm / $$aaaa

El solicitante declara que los datos expuestos son correctos.

PKI del Ministerio de Defensa

SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO

ENTIDAD EMISORA:

FECHA:	ERL EMISORA:
$$dd/$$mm/$$aaaa	$$raOperator

SUBSCRIPTOR O AGENTE:

E-MAIL:	DNI / PASAPORTE /TIM:
$$email	$$dni

NOMBRE:

$$givenName

APELLIDOS:

$$surname1 $$surname2

TIPOLOGÍA DE LOS CERTIFICADOS A REVOCAR:

TIPOLOGIA		
	X	Autenticación y Correo Electrónico ($$serialNumber.auth)

	X	Firma Electrónica ($$serialNumber.sign)
	X	Cifrado Digital ($$serialNumber.cipher)
		Servidor / Dispositivo / Otros
NIVEL	**$$ sw**	Nivel 2 (Software)
	$$ hw	Nivel 2 HW (Tarjeta Electrónica)

MOTIVO DE LA REVOCACIÓN:

$$revDetails

SERVIDOR / DISPOSITIVO / OTROS:

IDENTIFICADOR:

LOCALIZACIÓN:

FUNCIÓN:

Firma de Servidor	*Servidor Seguro*	*Dispositivo HW*	*Controlador de Dominio*	*Firma de Código*

El Operador de la ERL,	El Solicitante,
Fecha: $$dd / $$mm / $$aaaa	Fecha: $$dd / $$mm / $$aaaa
El operador de la ERL certifica que toda la información presentada es correcta y que cumple con las condiciones expresadas en la Política de Certificación de la PKI del Ministerio de Defensa.	El solicitante declara que los datos expuestos son correctos.