MINISTERIO
DE DEFENSA

SECRETARÍA DE ESTADO DE DEFENSA

DIRECCIÓN GENERAL
CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

CESTIC_NR_02_22

DECLARACION DE PRACTICAS DE CERTIFICACION DE LA PKI DEL MINISTERIO DE DEFENSA

24 de abril de 2024

Página intencionadamente en blanco

DOCUMENTO

METADATOS OBLIGATORIOS	
Categoría	Documento
Identificador	CESTIC_NR_02_22
Nombre	DECLARACION DE PRACTICAS DE CERTIFICACION DE LA PKI DEL MINISTERIO DE DEFENSA
Fechas	Fecha Fin: 24/04/24
Calificación	Tipo de valor: Administrativo Plazo de conservación: permanente
Características técnicas	Documento PDF (.pdf)
Tipo de Firma	Electrónica
Tipo documental	TD200
Estado de elaboración	EE02
Clasificación	2.07.02
Versión NTI	https://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e
Órgano	DIR3 (E04906002)
Origen del documento	CESTIC - DISEGINFO
Estado del documento	En vigor
Estado del expediente	N.A.
Interesado	Ministerio de Defensa
Nivel de seguridad	Uso Oficial

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 DPC 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 “grupo DIVOPER/PKI”.
1	9	03/11/2015	Revisión. Cambio SDGTIC por CESTIC. Actualización normativa.
2	0	01/12/2016	Revisión. Incorporación de la nueva jerarquía de certificación (SHA256). Cumplimiento requisitos ETSI 101456 y actualización conforme al Reglamento (UE) No 910/2014 (eIDAS). Adaptación de los perfiles de certificados al eIDAS y a los perfiles v2.0 de la AGE.
2	1	17/02/2017	Revisión. Modificaciones según comentarios recibidos del MINETAD para cumplimiento Reglamento (UE) No 910/2014 (eIDAS).
2	2	18/07/2017	Revisión, tras la notificación del MINETAD, para adaptar el documento y los perfiles de certificados tras la pérdida de consideración de “prestador de confianza cualificado” por el Ministerio de Defensa. Eliminación de toda referencia a “reconocido” o “cualificado”.

2	3	02/10/2018	Revisión, tras la notificación del MINCOTUR, para adaptar la DPC tras la inclusión del Ministerio de Defensa como "prestador de confianza cualificado" en la TSL. Incorporación de las referencias a certificados "cualificados" e inclusión de los perfiles nuevos. En concreto: • Punto 1.1: Adhesión expresa a CAB Forum. • Punto 2.1: Disponibilidad de certificados de ejemplo (válido, revocado, caducado). • Punto 4.9.3.1: Comprobación del estado de validez o revocación de un certificado más allá de su vigencia. • Punto 5.2.1.2: Comprobación periódica del estado de vigencia de la certificación de los HSM. • Punto 5.5.2: Corrección en el tiempo máximo que se conserva la información sobre certificados. • Punto 6.3.2: Periodo de validez de certificado de la EV: 1 año. • Punto 9.11: Cuenta de correo habilitada para la solicitud de certificados de prueba a la AGPMD. • Anexo2: Actualizado. • Anexo 4: Añadido Perfil de certificado OCSP. Anexo 8: Incluidas las plantillas de aceptación de certificados de sede, sello y dispositivo (emisión, renovación, revocación).
2	4	26/05/2020	Revisión. Añadido perfil TSA.
2	5	18/11/2020	Revisión: Modificado el perfil del certificado de firma de persona física, que se pasa a ser NO cualificado Modificado el servicio de validación de certificados: en vez de Valide, solo se contemplaPKIDEF. Modificado apartado 5.7.1: Notificacion en caso de incidente de seguridad. Modificado apartado 9.12.1: revisiones anuales de la DPC Modificado apartado 1.1: prevalencia del CAB Forum Modificado apartado 6.1.1: recomendación de generación de claves acorde a la ETSI Añadida Sección 4.2.6 "validación del control del dominio" Añadida Sección 4.2.7 "Registros AAC" Modificada Tabla 22: añadida la extensión obligatoria del CAB Forum para certificados de Autenticación de sitio web (QCP-W) Modificada Tabla 22: Añadidas dos extensiones nuevas para cumplir la normativa. Según la ETSI EN 411-1 GEN-6.3.3-12, para certificados EVCP (p.e QCP-w) se debe utilizar, al menos, una de las siguientes políticas: - El OID de la política EVCP de ETSI (0.4.0.2042.1.4). - El OID de la política EV de CABFORUM (2.23.140.1.1). - Un OID establecido por el TSP. Anexo 8: Eliminadas las plantillas de aceptación de certificados de sede, sello y dispositivo (emisión,

			renovación, revocación), ya que se contemplan en un documento aparte (Procedimiento de Solicitud de certificados). Introducidas referencias a la nueva Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
2	6	05/11/2021	Se modifica el apartado "9.6.3 Obligaciones de los subscriptores" para inlcuir la recomendación de que el par de claves generado en la TEMD se utilice sólo para firmas electrónicas. Se modifica el apartado 9.11 para indicar que el kit de certificados de prueba se debe solicitar a la dirección seginfo-pki@mde.es Se modifica la frecuencia de publicación de la ARL, de mensual a trimestral, en los apartados 2.3 y 4.9.3.1 Se incluye la extensíon OCSPNoCheck (1.3.6.1.5.5.7.48.1.5) como una extension independiente en vez de incluirla en el "Extended Key Usage" y se cambia el bit del "KeyAgreement" de 1 a 0. Apartado 4.1.1, Los operadores PKI será personal de DIVOPER/DISEGINFO. Apartado 4.7.3. Solo se permite renovar certificados online una vez. Anexo 2 (apartado 2.6.3): se modifica la caducidad del certificado de firma de código de 2 a 5 años
2	7	01/06/2022	Se modifica el apartado 6.5.2 "periodo de retención para el archivo" de 13 a 15 años después de haber expirado el certificado. Se modifica el apartado 10.6.4 "Obligaciones de Terceros Aceptantes". Se añade que es su responsabilidad comprobar que el PSC se encuentra en la lista TSL. Se modifica el apartado 5.10 "Servicios de comprobación de estado de certificados", indicando que PKIDEF dispondrá de un servicio de Last CRL en caso de compromiso de claves de las CAs así como en el caso de terminación y/ó cese de la actividad. De acuerdo con la RFC 3647 donde se indica que estructura debería seguir la DPC se añaden o modifican los siguientes apartados; a) 4.2.4 "Información no verificada del Subscriptor". b) 4.2.5 "Criterios para interoperación" c) Modificación del Aptdo 5.2 "Tramitación de la solicitud de certificados" con tiempo estimado de validar la solicitud. d) 5.7.7 "Notificación de la emisión del certificado por la CA a otras entidades" e) 6.1.8 "Respaldo externo" f) 7.2.10 "Clasificación de los módulos criptográficos"

			g) 10.3.3 "Responsabilidad para proteger información confidencial". h) 10.4 "Protección de datos personales". Modificación del apartado 5.7.3: el periodo de renovación se extendie a más de los 3 últimos meses de vigencia del certificado en determinadas circunstancias. Se modifica el perfil del certificado del certificado de autenticación web SSL (Anexo I), para eliminar el OU del Subject.
2	8	31/08/2022	La presente DPC se rige por la RFC 3647. Es por ello por lo que se proporciona un mapeo entre las funcionalidades definidas en la RFC con respecto a la presente DPC (ver Anexo VIII). Modificación del apartado 6.4.8 "Analisis de vulnerabilidades" indicando la gestión de las vulnerabilidades críticas en menos de 48 horas. Modificación del apartado 10.6.4 "Obligaciones de los Terceros Aceptantes". Modificado apartado 5.10, añadiendo que se publicará un Hash de la CRL en el caso de compromiso de clave y emitir una Last CRL. Modificado el perfil del certificado de firma de código (Anexo I, apartado 10.17.13) añadiendo a la extensión "KeyUsage" el campo "contentCommitment". Se ha modificado el perfil de los certificados de sede nivel alto y sede nivel medio añadiendo la extensión cabfOrganizationIdentifier (OID 2.23.140.3.1) en el Anexo I 10.17.4/5). Modificada la validez de los certificados de Sede (nivel alto y nivel medio de 24 meses a 12 meses: Anexo I 10.17.4/5). Modificados apartados 3.3 y 5.9.3.2, para justificar el periodo de refresco de las CRLs. Modificados los perfiles de los certificados de sede nivel alto y sede nivel medio con la extensión OID 2.23.140.1.1 (Anexo I 10.17.4/5). Modificada la validez del certificado de la EV (OCSP) de 12 a 6 meses en el Anexo III. Se eliminan todas las referencias al Portal de Renovación online o renovación remota, ya que no se ha podido poner en Producción por diferentes circunstancias. Se modifica el perfil del certificado del certificado de Sede Electrónica (Anexo I), para eliminar el OU del Subject.
2	9	23/04/2024	Se modifica la validez del certificado de firma de codígo para que no exceda de los 39 meses según indica el CABforum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (cabforum.org)

Contenido

FIGURAS

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[1]	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.
RFC 2251	Lightweight Directory Access Protocol (v3). http://www.faqs.org/rfcs/rfc2251.html

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

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.

2. INTRODUCCIÓN Y CONTEXTO.

2.1. 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 v1**), que permitiese la utilización de certificados electrónicos y el manejo de claves en entornos de alta seguridad. Con posterioridad, el Ministerio de Defensa ha adquirido tarjetas criptográficas (modelo comercial TC-FNMT) a la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, que está siendo evaluada según los requisitos certificación CC EAL4+ y perfil prEN 14169-1:2009, como evolución de su proyecto dispositivo de alta seguridad **TEMD v2** (con chip sin contactos Mifare), y **TEMD v3** (con chip sin contactos DESFIRE EV2).

El 29 de abril de 2009 el Ministerio de Industria, Turismo y Comercio (hoy Ministerio de Industria, Comercio y Turismo) dicta la resolución que, según la ley 59/2003 de firma electrónica, inscribe al Ministerio de Defensa en el registro de prestadores de servicios de certificación con certificados de firma. Con la entrada en vigor del Reglamento UE Nº 910/2014

(eIDAS), mediante una medida transitoria, se permitía temporalmente mantener esta consideración al Ministerio de Defensa para, únicamente, aquellos servicios en los que se expedían certificados cualificados de firma electrónica y que tenían consideración de certificados reconocidos con la legislación anterior. Sin embargo, no más tarde del 1 de julio de 2017, cualquier prestador de servicios de confianza (TSP) debía presentar ante el organismo de supervisión (Ministerio de Energía, Turismo y Agenda Digital) un informe de evaluación de la conformidad (CAR) auditando los servicios de confianza ya existentes (emisión de certificados de firma electrónica) así como cualquiera de los nuevos servicios definidos en eIDAS (emisión de certificados de sellos electrónicos, de certificados de autenticación de sitios web, sellado de tiempo, entrega certificada, validación y conservación). En consecuencia, en cumplimiento de la legislación comunitaria y hasta la presentación del correspondiente informe de evaluación CAR, a partir del 2 de julio de 2017 el Ministerio de Defensa pierde su condición de "cualificado" como entidad, así como todos los servicios que presta.

Una vez presentado el informe de evaluación CAR, recibida la aprobación por parte del Organismo supervisor (actual Ministerio de Industria, Comercio y Turismo) el día **20 de septiembre de 2018** y publicados los servicios cualificados ofrecidos por el Ministerio de Defensa en la Lista de Servicios de Confianza (TSL), se consideran como cualificados los siguientes servicios:

- Servicio de expedición de certificados electrónicos cualificados de firma electrónica:
  - Certificado cualificado de empleado público, nivel medio, firma electrónica.
- Servicio de expedición de certificados electrónicos cualificados de sello electrónico:
  - Certificado cualificado de sello electrónico de administración, órgano o entidad de derecho público, nivel medio;
  - Certificado cualificado de firma de sistema (sello electrónico), nivel medio/sustancial;
  - Certificado cualificado de firma de código, nivel medio/sustancial.
- Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web:
  - Certificado cualificado de sede electrónica, nivel alto;
  - Certificado cualificado de sede electrónica, nivel medio/sustancial;
  - Certificado cualificado de autenticación de sitios web, nivel medio/sustancial.

De esta forma, 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 cualificado** , dotando 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 consagró 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 siguieron a la Ley 11/2007 (Reglamento de desarrollo de la Ley 11/2007, Esquema Nacional de Seguridad y Esquema Nacional de Interoperabilidad) y finalmente, la Ley 39/2015 de Procedimiento Administrativo Común (que además deroga la anterior Ley 11/2007), se marca un objetivo claro de regular las relaciones entre las Administraciones y los ciudadanos en la que se tiene en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo este afecta a las relaciones entre Administraciones con ciudadanos y empresas.

La Ley 39/2015 da un giro importante a los procedimientos administrativos, ya que la tramitación electrónica es la principal siendo la excepción la tramitación en papel, y establece los perfiles comunes de los certificados digitales para que puedan interoperar en todas las Administraciones Públicas. Así, el Ministerio de Defensa elaboró y definió perfiles propios de Sede Electrónica, Sello Electrónico y Empleado Público para emitirlos 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.

Finalmente, tras la aprobación del Reglamento (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS), no se regulan únicamente los temas de firma electrónica, sino también los de identificación electrónica y otros servicios de confianza. Concretamente, regula los siguientes servicios:

- Firma electrónica
- Sello electrónico
- Marca de tiempo electrónica (sellado de tiempo)
- Documento electrónico
- Entrega electrónica
- Autenticación de sitio web

Este nuevo reglamento eIDAS es de obligado cumplimiento y no requiere de transposición en las diferentes legislaciones de cada Estado Miembro sobre firma electrónica.

En este sentido, 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.

Según lo anterior y cumpliendo con los estándares internacionales vigentes (RFC 3647, ETSI EN 319 411-1), esta Declaración de Prácticas de Certificación (DPC) detalla las normas y condiciones generales de los servicios de certificación del Ministerio de Defensa, para 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 los

certificados, las medidas de seguridad técnicas y organizativas, perfiles y mecanismos de información sobre la vigencia de los certificados.

De esta forma, la presente DPC recoge las normas aplicables a la actividad del Ministerio de Defensa como Prestador de Servicios de Confianza 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 para los servicios de certificación ofrecidos:

- *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 del grupo DIVOPER/PKI, dependiente de la Unidad de Sistemas de ACESIN, 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”. Para dotar de carácter uniforme al documento y facilitar su lectura y análisis, se incluyen 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 y europea. Explícitamente se asumen como de aplicación obligatoria las siguientes normas:

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- 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 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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 artículo 23 del 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 confianza, 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 confianza 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.

Por último, la presente DPC cumple con lo especificado en las guías "*Guidelines For The Issuance And Management Of Extended Validation (EV) Certificates*" elaboradas por *Certification Authority Browser Forum (CAB Forum)*. En el caso de discrepancia entre ambas prevalecerán las guías del CAB Forum en su última versión.

2.2. Nombre del Documento de Identificación

La siguiente tabla de identificación aplica al presente documento:

Nombre	Declaración de Prácticas de Certificación (DPC) de la PKI de la Red de Propósito General del Ministerio de Defensa.
Versión	2.8
Estado	Revisada y Aprobada
Fecha Emisión / Fecha Caducidad	02/08/2022 02/08/2023.
OID	2.16.724.1.1.1.1.3.0.1
Ubicación	https://www.defensa.gob.es/pki/dpc/

Ilustración 1: Identificación DPC de la PKI de la Red de Propósito General 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).

2.3. 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.

2.3.1. 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.

2.3.2. Entidad de Certificación

Las Entidades de Certificación que componen PKIDEF son: La Entidad de Certificación Raíz (DEFENSA-EC-RAIZ) y una Entidad de Certificación Subordinada (DEFENSA-EC-WPG2016), cuyos datos se muestran a continuación. Ambas están adaptadas completamente a los últimos requisitos y estándares criptográficos demandados a nivel nacional e internacional. En tal medida, que todos los certificados digitales que se emitan (de personas, sistemas y dispositivos) tendrán claves RSA de 2048 bits y estarán firmados con la función resumen SHA-256, dejando de emitirse los certificados con tamaño de claves de 1024 bit y función resumen SHA-1 utilizados anteriormente.

EC RAÍZ (DEFENSA-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. Es un certificado auto-firmado y posee las claves de la EC-Raíz anterior (MINISDEF-EC-RAIZ).

Emisor	CN = DEFENSA-EC-RAIZ organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Titular	CN = DEFENSA-EC-RAIZ organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Número de Serie	6f 25 57 fe 6b 89 ef b5 57 c9 5b 5a 0c 98 ce 33
Periodo de Validez	viernes, 2 de septiembre de 2016 11:58:34 viernes, 8 de noviembre de 2041 13:00:00
Función resumen del certificado.	Sha1 93 a0 36 bc 0e fa b4 c8 34 27 69 94 d2 49 7a af c0 dd 00 ed
Algoritmo de firma	sha256RSA

Ilustración 2: Identificación DEFENSA-EC-RAIZ

EC SUBORDINADA (DEFENSA-EC-WPG2016)

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

Emisor	CN = DEFENSA-EC-RAIZ organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Titular	CN = DEFENSA-EC-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Número de Serie	4e 42 ea 0d a1 c2 c1 3f 57 d1 18 7f fa ed 2f 1e
Periodo de Validez	jueves, 8 de septiembre de 2016 8:51:27 miércoles, 8 de septiembre de 2027 8:51:27
Función resumen del certificado.	Sha1 b2 12 44 8e 6a 21 f3 3d d9 a1 f0 51 d3 89 ef 52 3d 72 c8 09
Algoritmo de firma	sha256RSA

Ilustración 3: Identificación DEFENSA-EC- WPG2016

2.3.3. Entidad de Registro

Las entidades de registro de PKIDEF las componen, conjuntamente, los servicios telemáticos que permiten la gestión de vida de los certificados centralizada a los subscriptores y los puestos de expedición presencial que operan en las localizaciones del Ministerio de Defensa al territorio nacional. 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 renovación o revocación de estos, de manera no presencial.
- Entidad de Registro Local (ERL): dedicada al registro de peticiones de certificación de los subscriptores, así como la solicitud de la renovación o revocación de sus certificados ya emitidos, de manera presencial. También permite la solicitud de certificados para dispositivos y sistemas del Ministerio de Defensa a los administradores o responsables.

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 por la ER se identifican mediante los siguientes datos:

Emisor	CN = DEFENSA-EC-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Titular	CN = DEFENSA-ER03-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA

	C = ES
Número de Serie	4e aa 57 6e fc 78 b1 09 5b 98 d2 f4 d9 c4 ba 2b
Periodo de Validez	miércoles, 12 de septiembre de 2018 9:48:52 viernes, 11 de septiembre de 2020 23:00:00
Función resumen del certificado.	Sha1 eb 8d 52 7d e3 b2 c0 63 30 1e 02 c2 fb cd 4b 56 3b 02 fb 01
Algoritmo de firma	sha256RSA

Ilustración 4: Identificación DEFENSA-ER03-WPG2016

Emisor	CN = DEFENSA-EC-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Titular	CN = DEFENSA-ER04-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Número de Serie	76 ed 7f aa d6 d1 88 53 5b 98 d3 6a f6 f5 65 62
Periodo de Validez	miércoles, 12 de septiembre de 2018 9:50:50 viernes, 11 de septiembre de 2020 23:00:00
Función resumen del certificado.	Sha1 3c 87 ab 0a 6a d9 24 e4 a9 28 d0 32 9d e9 16 d8 4f 24 a3 ba
Algoritmo de firma	sha256RSA

Ilustración 5: Identificación DEFENSA-ER04-WPG2016

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 tienen un certificado propio como entidad de PKIDEF, sino que se identifican y autorizan con el 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, mediante un proceso de registro presencial que garantice la correcta identificación del solicitante de certificados y la entrega de estos al momento de la solicitud.

2.3.4. 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 DEFENSA-EC-WPG2016.

La Entidad de Validación realiza su labor conforme a la RFC 2560: X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol (OCSP). Así, la EV del Ministerio de Defensa presta servicios OCSP para 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 = DEFENSA-EC-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Titular	CN = DEFENSA-EV-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Número de Serie	32c88f0183fe4ebf65e833607b0364fe
Periodo de Validez	6 meses
Función resumen del certificado.	Sha1 830db80a99996b9120850b496a34b2dafb952709
Algoritmo de firma	sha256RSA

Ilustración 6: Identificación DEFENSA-EV-WPG2016

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

http://ev.mde.es

2.3.5. 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 de este. 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 del grupo DIVOPER/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 = DEFENSA-EC-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Titular	CN = DEFENSA-EST-WPG2016 organizationIdentifier = VATES-S2800231I OU = PKI O = MINISTERIO DE DEFENSA C = ES
Número de Serie	7a2077f4d0868f275e2832add490dc7e
Periodo de Validez	miércoles, 22 de enero de 2020 13:31:57 miércoles, 22 de enero de 2025 1:00:00
Función resumen del certificado.	Sha1 6081ba6465ea7106f849c0b6c5acb04bbae28a4a
Algoritmo de firma	sha256RSA

Ilustración 7: Identificación DEFENSA-EST-WPG2016

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

http://est.mdef.es

2.3.6. 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 DEFENSA-EC-WPG2016.
- 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 muy importante la Aplicación de Gestión de Tarjetas (AGT), operada en exclusiva por el personal del grupo DIVOPER/PKI.

2.3.7. Entidades Finales

2.3.7.1. Subscriptores

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 del Ministerio de Defensa, notificado por el canal de comunicación pertinente a presentarse en un Puesto de Gestión de Tarjetas (PGT) y después 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). Solo 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 quien lo administrará. 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 subscriptores de PKIDEF, el término subscriptor se empleará solo para las entidades que soliciten certificados para usos diferentes a los de emisión y firma de certificados y CRL.

2.3.7.2. 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 solo darán, como íntegras y confiables, las transacciones firmadas y validadas por otros usuarios del Ministerio de Defensa mediante los servicios de validación y sellado temporal desplegados por el Ministerio de Defensa o 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 esta por parte de la AGPMD a través de

los mecanismos de comunicación pertinentes en cada centro de explotación del Ministerio de Defensa.

2.4. 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:
  - Autenticación Web (SSL/TLS): OID 2.16.724.1.1.1.1.2.7 (cualificado)
  - Dispositivo Seguro: OID 2.16.724.1.1.1.1.2.5
  - Controlador de Dominio: OID 2.16.724.1.1.1.1.2.15
  - Identificación de Dispositivo: OID 2.16.724.1.1.1.1.2.16
  - Firma de Código: OID 2.16.724.1.1.1.1.2.6 (cualificado)
  - Firma Sistema (Sello): OID 2.16.724.1.1.1.1.2.8 (cualificado)
  - Identificación Sistema: OID 2.16.724.1.1.1.1.2.9
  - Sede Electrónica Nivel Medio: OID 2.16.724.1.1.1.1.2.10 (cualificado)
  - Sello Electrónico Nivel Medio: OID 2.16.724.1.1.1.1.2.14 (cualificado)
- **Clase 2 hardware:** para personas, dispositivos y sistemas cuya clave privada se haya generado en un dispositivo hardware:
  - Autenticación Persona Física: OID 2.16.724.1.1.1.1.3.1
  - Firma Persona Física: OID 2.16.724.1.1.1.1.3.2
  - Cifrado Persona Física: 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
  - 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 (cualificado)
  - Cifrado Empleado Público: OID 2.16.724.1.1.1.1.3.13
  - Sede Electrónica Nivel Alto: OID 2.16.724.1.1.1.1.3.10 (cualificado)

La descripción en detalle de cada perfil de certificado puede encontrarse en el Anexo I 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 39/2015 y la normativa relacionada posterior.
- **Sistemas del Ministerio de Defensa relacionados con sistemas externos de otros Ministerios, Administraciones, organismos u organizaciones externas autorizados previamente por la AGPMD.**
- **Sistemas externos de otros Ministerios, Administraciones, organismos u organizaciones 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 estos 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.

2.4.1. Usos prohibidos

No se permite el uso de certificados fuera del ámbito descrito en esta DPC, pudiendo revocar inmediatamente los certificados por su uso indebido.

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 activarse ni entregarse a un usuario del Ministerio de Defensa sin sus certificados personales.

2.5. Gestión de la Declaración de Prácticas de Certificación

2.5.1. Especificación de la Organización Administradora

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

2.5.2. 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 **Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones**, con dirección de contacto: C/ Arturo Soria 289, Teléfono 91 395 4400.
- Responsable del grupo DIVOPER/PKI: Referenciado en el presente documento como **Responsable del grupo DIVOPER/PKI** con dirección de contacto: C/Arturo Soria 289, Teléfono 91 395 4436.
- Responsable de Seguridad Física de ACESIN: Está representado por el **Jefe de la Oficina de Seguridad del Complejo Arturo Soria 289** con la siguiente dirección de contacto: C/ Arturo Soria 289, Teléfono 91 395 4689.
- Entidad de Control de Nombres (**ECN**): Representado por el **Responsable de la Subunidad de Servicios de Seguridad de Infraestructura y S.O. Cliente de DIVOPER**, con dirección de contacto C/ Arturo Soria 289, Teléfono 91 395 4405.

2.5.3. 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.

Si el grupo DIVOPER/PKI no puede operar en las condiciones establecidas en esta DPC, no dará servicio hasta la autorización expresa de operación de la AGPMD una vez estudiadas las condiciones reales de operatividad del grupo DIVOPER/PKI.

2.5.4. Acrónimos

ACRÓNIMO	*SIGNIFICADO*
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.
ACESIN	Área Central de Sistemas de Información
CESTIC	**Ce**ntro de **S**istemas y **T**ecnologías de la **I**nformación y las **C**omunicaciones
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
DIVOPER	División Operaciones en Red del CESTIC
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.
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. Denominación genérica para los diferentes modelos físicos existentes (TEMD v1 fabricada por Microelectrónica Española, TEMDv2 fabricada por FNMT-RC,…)
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

3. PUBLICACION DE INFORMACION Y REPOSITORIO DE CERTIFICADOS

3.1. 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.mde.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 https://www.defensa.gob.es/pki. Permite el acceso a la información publicada por PKIDEF, incluidos ejemplos de certificados válidos, revocados y caducados.

3.2. 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:

https://www.defensa.gob.es/pki/dpc/

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:

https://www.defensa.gob.es/pki/ca/DEFENSA-EC-RAIZ.crt

https://www.defensa.gob.es/pki/ca/DEFENSA-EC-WPG2016.crt

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:

https://www.defensa.gob.es/pki/crl/DEFENSA-CRL-EC-RAIZ.crl

https://www.defensa.gob.es/pki/crl/DEFENSA-CRL-EC-WPG2016.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).

3.3. Frecuencia de publicación

La presente DPC se publicará en su creación y se volverá a publicar cuando se apruebe cualquier modificación sobre la misma. Todos los cambios en el documento deberán ser aprobados por la AGPMD.

Los certificados emitidos por PKIDEF se publican en DICODEF tras la finalización exitosa del proceso generación o renovación, 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 manualmente y con un periodo de tres meses, si no hay 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 un periodo aproximado de hasta **5 minutos,** debido a las complejidades de la red del MDEF. Es por ello por lo que se sugiere que, por fiabilidad, se utilice el método de validación por OCSP.

3.4. 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 DEFENSA-EC-WPG2016) 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.

4. IDENTIFICACIÓN Y AUTENTICACIÓN

4.1. Registro Inicial

4.1.1. Tipos de nombres

DEFENSA-EC-WPG2016 generará y firmará certificados que contengan un nombre distintivo (Distinguished Name o DN) conforme con el estándar X.501, en el campo “SUBJECT NAME”. DEFENSA-EC-WPG2016 utilizará los DN de los subscriptores que les hayan sido asignados en DICODEF por la Entidad de Control de Nombres del Ministerio de Defensa.

No se contempla el uso de pseudónimo.

4.1.2. Asignación de nombres

No es responsabilidad de DEFENSA-EC-WPG2016 la asignación de nombres, asumiendo la existencia de estos en DICODEF mediante la aprobación previa de la Entidad de Control de Nombres (ECN) y los responsables del directorio.

4.1.3. Reglas para interpretar varios formatos de nombres

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

DEFENSA-EC-WPG2016 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.

4.1.4. Unicidad de los nombres

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

4.1.5. Procedimientos de resolución de disputas de nombres

No es responsabilidad de DEFENSA-EC-WPG2016 o las ER resolver sobre disputas de nombres, debiendo haber sido resueltas previamente por la ECN, que opera DICODEF.

4.1.6. Reconocimiento, autenticación y función de las marcas registradas

No estipulado.

4.2. Validación Inicial de la Identidad

4.2.1. 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 DEFENSA-EC-WPG2016 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 se introducen en su tarjeta. Como medida de seguridad adicional se comprueba que la tarjeta en la que se introducen los certificados es la que tiene asignado el subscriptor.
- El par de claves del certificado de firma se generan en la tarjeta TEMD, dispositivos diseñados y fabricados 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 DEFENSA-EC-WPG2016 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.

4.2.2. Autenticación de la identidad de una organización

En aquellos casos en los que PKIDEF emite certificados para un organismo del Ministerio de Defensa, como el caso de los Sellos Electrónicos, la solicitud deberá ser realizada por un representante autorizado del organismo, debiendo aportar durante el proceso el documento de nombramiento u otro documento de apoderamiento o equivalente.

4.2.3. Autenticación de la identidad de un individuo

4.2.3.1. Certificados de persona

4.2.3.1.1. 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, renovación 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 ésta 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 documentación, en soporte electrónico, 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.

Al firmar dicha documentación electrónica, el usuario acepta las condiciones de uso de los certificados y se somete a lo estipulado en esta DPC sobre sus condiciones.

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

4.2.3.2. 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 DEFENSA-EC-WPG2016 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 ante una ERL, usando la TEMD y el certificado de autenticación del Agente. El Agente de la PKI deberá autorizarse como Operador de Registro para la tipología solicitada de certificado.
- Mediante un correo firmado por el propio Agente PKI enviada al grupo DIVOPER/PKI.
- Mediante una solicitud formal a través del sistema de gestión de incidencias del Ministerio de Defensa (SCANS) dirigida al grupo DIVOPER/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.

Se guarda documentación, en soporte electrónico, de dicha solicitud que permite la identificación del Agente PKI. Debe contener, al menos, la siguiente documentación:

- La identidad de la persona que recibe la información y realiza la identificación.
- Una declaración firmada del Agente PKI y por 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.

Al firmar dicha documentación electrónica, el Agente PKI acepta las condiciones de uso de los certificados y se somete a lo estipulado en esta DPC sobre sus condiciones de uso.

4.2.4. Información no verificada del Subcriptor.

Toda la información incorporada al Certificado electrónico es verificada por la Autoridad de Registro / Personal de PKIDEF, por tanto, no se incluye información no verificada en el campo "Subject" de los certificados expedidos.

4.2.5. Criterios para interoperacion.

No existen relaciones de interactividad con Autoridades de Certificación externas a PKIDEF.

4.2.6. Validación del control del dominio

Para validar el dominio de los Certificados de autenticación de sitios web, la PKIDEF utiliza alguno de los siguientes métodos descritos en el documento CA/Browser Forum's Baseline Requirements: "3.2.2.4.6 Agreed-Upon Change to Website" ó "3.2.2.4.7 DNS Change". Para cada uno de los métodos empleados, la PKIDEF seguirá un proceso documentado y mantendrá registros que indiquen los métodos empleados para cada emisión. El resto de los métodos descritos en CA/Browser Forum's Baseline Requirements no se emplea para la validación de dominios.

4.2.7. Registro AAC

Registro AAC (CAA records): Registro de recursos DNS (Sistema de Nombres de Dominio) de Autorización de Autoridad de Certificación (AAC). Permite a un titular de nombre de dominio DNS especificar las Autoridades de Certificación (AC) autorizadas para emitir certificados para ese dominio. La publicación de los registros de recursos de AAC permite a un titular de nombres de dominio implementar controles adicionales para reducir el riesgo de que se produzca una emisión no autorizada de un Certificado de autenticación de sitios web para su nombre de dominio.

La PKIDEF comprueba si hay un Registro AAC para cada nombre de dominio que incluye en un Certificado de autenticación de sitios web emitido, de acuerdo con el procedimiento establecido en RFC 8659 y siguiendo las instrucciones de procesamiento establecidas en RFC 8659 para cualquier registro encontrado. Si existe dicho Registro AAC, la PKIDEF emitirá certificado para ese dominio siempre y cuando el literal "mde.es" aparezca en el registro AAC como entidad de certificación autorizada a emitir certificados para ese dominio. Si el Registro AAC no está disponible cualquier entidad de certificación está autorizada a emitir certificados para dicho dominio.

4.3. Identificación y autenticación en las solicitudes de renovación

Se entiende por renovación simple en este documento (o simplemente renovación[2]) 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 reemisión ni la actualización de certificados. En los casos que aplicará, se procederá a la

[2] Durante el presente documento se podrán encontrar los términos renovación simple o renovación como términos análogos, al ser el único método permitido por la presente DPC.

revocación de los certificados y a la generación de los nuevos en las condiciones vigentes del solicitante.

4.3.1. Procedimiento de rutina para la Renovación Simple de un certificado

La renovación simple 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.

4.3.2. Procedimiento de Renovación Simple de un certificado después de una Revocación

El procedimiento de renovación simple 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.

4.4. Identificación y autenticación en las solicitudes de revocación

Todas las solicitudes de revocación deberán estar autenticadas.

4.4.1. 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 revocará eficazmente si detecta inconformidad con lo expresado. En caso de disputa debe remitirse el caso al grupo DIVOPER/PKI.

5. EL CICLO DE VIDA DE LOS CERTIFICADOS

5.1. 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 el mensaje o correo que acredite la posesión del “PIN de Usuario” (nomenclatura específica de la AGT, responsable de la distribución de este) y un medio de identificación válido según lo descrito en la sección *4.2.3* Autenticación de la identidad de un individuo (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, 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.

5.1.1. 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 *4.2.3* Autenticación de la identidad de un individuo.

En el caso de certificados de dispositivo o sistema, el Agente de la PKI (personal de DIVOPER/DISEGINFO) se autenticará como Operador de la ERL con su tarjeta TEMD y generará él mismo el registro de solicitud, siguiendo lo estipulado en la *sección 4.2.3* Autenticación de la identidad de un individuo.

Todas las comunicaciones entre las Entidades de Registro (ER y ERL) que dan servicio a las solicitudes y DEFENSA-EC-WPG2016 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.

5.1.2. Entrega de la clave pública del subscriptor al emisor del certificado

Para los certificados personales, la clave pública del certificado de cifrado la genera DEFENSA-EC-WPG2016 (emisor del certificado), momento en que obtiene una copia de esta, de manera que se considera entrega efectiva de la clave el momento de la generación. La clave pública de los certificados de autenticación y firma, la genera el subscriptor en la tarjeta TEMD. DEFENSA-EC-WPG2016 la recupera en el momento de construcción del certificado, de manera que se considera la entrega efectiva de las claves el momento de construcción del certificado. Así, las claves públicas las entrega el subscriptor a la EC Subordinada (DEFENSA-EC-WPG2016) al firmar la 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). DEFENSA-EC-WPG2016 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 (DEFENSA-EC-WPG2016) en el momento de aceptación del PKCS#12.

5.2. 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 4 de la presente DPC.

El plazo de tiempo en procesar la solicitud de un Certificado depende en gran medida de que el Representante del Suscriptor proporcione la información y la documentación necesarias de la forma prevista en los procedimientos aprobados por la PKIDEF para este fin. No obstante, esta Entidad hará el esfuerzo necesario para que el proceso de validación que dará como resultado la aceptación o el rechazo de la solicitud no excedan de tres (3) días hábiles.

Este periodo podrá superarse ocasionalmente por motivos fuera del control de la PKIDEF. En estos casos, hará lo posible por mantener informado al Representante del Suscriptor que realizó la solicitud de las causas de tales retrasos.

5.3. Emisión de Certificados

Una vez que se reciba la solicitud de un certificado, DEFENSA-EC-WPG2016 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 DEFENSA-EC-WPG2016, de forma que ésta pueda comprobar la integridad de estas. Además, DEFENSA-EC-WPG2016 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, DEFENSA-EC-WPG2016 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. Si se informa sobre la inexactitud o la no aplicabilidad actual de la información contenida en el certificado, se puede revocar.

5.3.1. Entrega de la clave privada a los subscriptores

Para los certificados personales, la clave privada del certificado de cifrado se genera en la EC Subordinada y se entrega al usuario previa introducción por parte de este 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 a los certificados de autenticación y firma se genera en la TEMD del usuario previa introducción por parte de este del PIN que faculta el acceso a la parte privada de su tarjeta. El usuario final no debe aceptar otra forma de distribución de las

claves privadas que la descrita en esta DPC, debiendo introducir personalmente el PIN, asegurando la confidencialidad del proceso.

5.3.2. 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 conocerá la emisión del certificado cuando recibe una respuesta positiva a su solicitud, recibiendo el fichero PKCS #12.

5.3.3. Distribución de la clave pública de la EC a los usuarios de PKIDEF

La clave pública de DEFENSA-EC-WPG2016 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.

5.4. 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 10.6.3* Obligaciones de los subscriptores.
- Informar al subscriptor que se ha generado un certificado y los contenidos de este.
- Requerir del subscriptor la aceptación tanto de sus obligaciones como del certificado, mediante la firma electrónica del Documento de Aceptación[3].

La aceptación de los certificados por parte de los subscriptores se produce al firmar el Documento de Aceptación, que implica conocer y aceptar por parte del subscriptor de esta DPC y sus obligaciones.

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

5.4.1. Publicación del certificado por la EC

Los certificados emitidos por DEFENSA-EC-WPG2016 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”.

5.4.2. 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 se da al activar y generar los certificados, que se publican inmediatamente en la entrada de DICODEF correspondiente al Nombre Distintivo (DN) del titular.

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

5.5. Uso del Par de Claves y de los Certificados

5.5.1. 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 sitios web
  - Autenticación de dispositivos, servidores, routers, firewalls, etc.
  - Autenticación de sistemas y aplicaciones.
  - Autenticación de controladores de dominio Windows
- **Certificados de Firma Electrónica**:
  - 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.
- **Certificados de Sello Electrónico**:
  - Sello Electrónico para la actuación administrativa automatizada.
  - Firma (sello electrónico) de sistemas y aplicaciones
  - Firma (sello electrónico) 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.

5.5.2. 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.

5.6. Renovación de Certificados sin 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 su certificado sin cambiar su clave privada.

La DPC no contempla el proceso de reemisión, así que la renovación de claves implica la renovación de certificado y no se puede hacer como procesos separados.

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

5.7. Renovación de Certificados con 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 el certificado y su clave privada.

5.7.1. Circunstancias para una renovación simple

La presente DPC establece los siguientes motivos de renovación simple 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 renovación del certificado. PKIDEF enviará el correo electrónico al subscriptor con la dirección publicada en DICODEF, en la entrada correspondiente al subscriptor.

5.7.2. Quién puede pedir la renovación simple de un certificado

La renovación simple 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.

5.7.3. Tramitación de las peticiones de renovación simple de certificados

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

La renovación simple de los certificados personales únicamente 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 renovación presencial es la misma que para su emisión inicial descrito en la *sección 4.2.3.1.1 Autenticación presencial*.

Asimismo, el procedimiento de renovación 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 renovación 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 renovación de un certificado cada 2 años, dentro de sus últimos 3 meses de vigencia (salvo determinadas circunstancias que este periodo podrá ser superior si es debidamente justificado).
- Que la solicitud de renovación se refiera al mismo tipo de certificado emitido inicialmente.
- Durante la renovación, PKIDEF controla que el certificado esté en los últimos 3 meses de vigencia (salvo ciertas circunstancias que este periodo podrá superar si se justifica debidamente) y que el nuevo 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.

5.7.4. Notificación de la renovación simple de un certificado al subscritor

Los subscriptores son conscientes de la renovación del nuevo certificado al recibir su tarjeta TEMD con los nuevos certificados personales.

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.

5.7.5. Pautas de aceptación del nuevo certificado

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

5.7.6. Publicación del nuevo certificado por la EC

Los certificados renovados por DEFENSA-EC-WPG2016 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.

5.7.7. Notificación de la emisión del certificado por la CA a otras entidades

PKIDEF notificará la renovación de los certificados emitidos a otras entidades externas, mediante el mecanismo proporcionado por dichas entidades. Así, por ejemplo, para el caso del certificado de la TSA de la plataforma @FIRMA, se notifica mediante la web dispuesta por la SGAD: https://ssweb.seap.minhap.es/ayuda/consulta/CAID

5.8. 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.

Esta DPC no contempla la actualización de certificados, así que, en los casos que aplicará, se revocarán los certificados y se generarán los nuevos en las condiciones vigentes del solicitante.

5.9. Suspensión y Revocación de Certificados

5.9.1. Suspensión

No se contempla la suspensión de certificados.

5.9.2. Revocación

5.9.2.1. Circunstancias para la revocación

La revocación de un certificado es por el que se deja sin efecto la validez de un certificado antes de caducidad. El efecto de la revocación de un certificado es la pérdida de vigencia de este, originando el cese permanente de su operatividad según los usos propios y de la prestación de los servicios de certificación. La revocación de un certificado impide el uso de este 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 está sujeto a baja prolongada por causa mayor, según la normativa del Ministerio de Defensa o Legislación Española vigente al aplicar y vigencia de esta DPC.
- Que exista sospecha de compromiso de la clave privada o ésta se revela como “débil”.

- Que el subscriptor o el responsable del grupo DIVOPER/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 confianza salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos sea transferidos a otro prestador de servicios de confianza.
- Resolución judicial o administrativa que lo ordene.
- Cualquier otra aprobada en exclusividad por la AGPMD o establecida en el artículo 5 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Para cualquiera de las circunstancias descritas anteriormente se rellenará el formulario[4] correspondiente aprobado y publicado a tal fin por la AGPMD.

La revocación afecta al certificado la terminación inmediata y anticipada de su periodo de validez, deviniendo el certificado como no válido. La revocación no afectará a las obligaciones subyacentes creadas o comunicadas por esta DPC ni tendrá efectos retroactivos.

5.9.2.2. Quién puede solicitar la revocación

DEFENSA-EC-WPG2016 podrá revocar certificados siempre y cuando haya sido el emisor y esté autorizada la revocación por el responsable del grupo DIVOPER/PKI. En el caso de revocación de Entidades propias de la PKI y revocaciones masivas es potestad exclusiva del grupo DIVOPER/PKI.

El operador de la ERL podrá solicitar la revocación del certificado de un subscriptor, representando a las personas autorizadas en esta DPC, si sospechase del compromiso de la clave privada del subscriptor, o cualquier hecho determinante que recomendará emprender dicha acción.

Los usuarios finales y Agentes de la PKI (personal de DIVOPER/DISEGINFO) 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.

5.9.2.3. Procedimiento de solicitud de revocación

DEFENSA-EC-WPG2016 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 relleno y firma el formulario aprobado para este fin por la AGPMD.

[4] *Ver* ***¡Error! No se encuentra el origen de la referencia.****Anexo VII.*

-
- El Agente de la PKI (personal DIVOPER/DISEGINFO) solicita la revocación de un certificado de dispositivo o sistema de forma a través de la ERL. Tras la comprobación positiva de la identidad del Agente de la PKI (la autenticación en la ERL se hace mediante su certificado de autenticación, que debe seguir vigente en fecha y que no se haya revocado), la solicitud de revocación se generará y firmará el Agente de la PKI representando al 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 DEFENSA-EC-WPG2016. Todas las solicitudes deberán estar autenticadas; para aquellas firmadas por el subscriptor o por la ER, con la verificación de la firma será suficiente.

DEFENSA-EC-WPG2016, 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, DEFENSA-EC-WPG2016 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.

5.9.2.4. 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* *5.9.3.1* Frecuencia de emisión de las CRL.

5.9.2.5. 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 los casos, se establece un plazo de 6 horas para la tramitación desde la notificación de la solicitud de revocación.

5.9.3. Listas de Certificados Revocados

Las listas de certificados revocados se publican en DICODEF:

cn=DEFENSA-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES, para la ARL.

cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES, para la CRL

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

https://www.defensa.gob.es/pki/crl/DEFENSA-CRL-EC-RAIZ.crl, para la ARL.

https://www.defensa.gob.es/pki/crl/DEFENSA-CRL-EC-WPG2016.crl, para la CRL

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

5.9.3.1. 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.

La ARL se publica mediante procedimientos manuales a cargo exclusivo del personal del grupo DIVOPER/PKI, con una frecuencia trimestral.

5.9.3.2. Tiempo máximo entre la generación y la publicación de las CRL

La publicación de las CRL en los repositorios se realiza en un periodo aproximado de hasta 5 minutos, debido a las complejidades de la red del MDEF.

5.9.3.3. 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 a cada uso y descargarse la nueva CRL de los repositorios habilitados por el Ministerio de Defensa tras el periodo de validez de la que posean.

5.9.4. 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.

Cumpliendo con lo establecido en el artículo 24.4 del Reglamento eIDAS, el estado de validación o revocación de un certificado se pone a disposición de cualquier usuario incluso después de su período de validez a través del servicio de validación OCSP de PKIDEF.

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

http://ev.mde.es

El servicio de validación se basa en consultas al estado de las bases de datos de DEFENSA-EC-WPG2016, según parámetros de validez configurables, para asegurarse una respuesta precisa del estado del certificado al momento de su consulta.

5.9.4.1. 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 estos.

5.9.5. 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 verificar los certificados solo se admitirá como método alternativo, en caso de problemas técnicos en el acceso a la Entidad de Validación o cuando el sistema trabaje aislado.
- La autorización, de forma excepcional, para el uso de CRL como método exclusivo de verificación es potestad de la AGPMD.
- Si accederán a la ARL, comprobando su validez y haciéndose uso en la comprobación de la cadena de validación completa.

5.9.6. Otras formas de divulgación de información de revocación disponibles

No estipulado.

5.10. 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.

En el caso de compromiso de las claves de la CA Raiz o de la Subordinada, o en el caso de terminación y/ó cese del PSC se dispondrá de un servicio de Last CRL (con fecha de validez 9999), donde las aplicaciones cliente podrán consultar el estado de los certificados más allá de su vida útil. Si hubiese un compromiso de clave se facilitará/publicará un hash de la CRL en el Portal PKI (https://www.defensa.gob.es/pki).

5.11. Finalización de la suscripción

La suscripción (relación entre el subscriptor y la DEFENSA-EC-WPG2016) finaliza con la expiración o revocación del certificado.

5.12. Custodia y recuperación de claves

La presente DPC sólo permite la custodia 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.

DEFENSA-EC-WPG2016 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. Esto es una muestra de texto de estilo normal, que se utilizará a lo largo de todo el documento.

6. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y OPERACIONALES

6.1. Controles de Seguridad Física

6.1.1. 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.

6.1.2. Acceso físico

El Centro de Proceso de Datos del Ministerio de Defensa (situado en el CESTIC) dispone de diferentes perímetros de seguridad, con diferentes requerimientos de seguridad y autorizaciones. La presente DPC delega los controles de acceso físico a la Oficina de Seguridad del Complejo Arturo Soria 289.

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 de DIVOPER bajo los criterios de seguridad definidos por la División citada anteriormente.

La posesión y custodia de las llaves de acceso físico a los sistemas de PKIDEF es exclusiva del personal del grupo DIVOPER/PKI.

6.1.3. 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 se compone de equipos independientes con capacidad para mantener niveles de temperatura y humedad en los márgenes de operación óptimos de los sistemas.

6.1.4. 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.

6.1.5. 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.

6.1.6. 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.

6.1.7. Eliminación de residuos

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

6.1.8. Respaldo externo

PKIDEF dispone de una infraestructura de respaldo en una localización externa para la recuperación en caso de desastre (véase apartado 6.7.4 “Recuperación en caso de desastre”).

6.2. Controles de Procedimiento

6.2.1. Perfiles de confianza

En general, todos los perfiles definidos en PKIDEF serán personal del CESTIC, no pudiendo solapar sus funciones en aquellos roles excluyentes.

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

6.2.1.1. 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 (DEFENSA-EC-RAIZ, DEFENSA-EC-WPG2016, DEFENSA-ER03-WPG2016, DEFENSA-ER04-WPG2016, DEFENSA-EV-WPG2016 y DEFENSA-EST-WPG2016).

6.2.1.2. 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 DEFENSA-EC-RAIZ y DEFENSA-EC-WPG2016.
- 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 HSM SafeNet Luna G5, asociado a la EC Raíz es labor exclusiva del grupo DIVOPER/PKI.
  - La operativa de los módulos Realsec Cryptosec LAN, asociados al resto de entidades de PKIDEF (EC Subordinada, ER, EV y EST) es responsabilidad del personal del grupo DIVOPER/PKI.
- Verifica periódicamente que la certificación de los HSM sigue vigente. Si se pierde por cualquier motivo, se sustituirá los modelos actuales por otros certificados.

6.2.1.3. 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.

6.2.1.4. Oficial de Registro

Es el responsable de la gestión del ciclo de vida de cualquier certificado emitido por la EC Raíz y la EC Subordinada, 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 (DEFENSA-EC-RAIZ o DEFENSA-EC-WPG2016).
- 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.

6.2.1.5. Operador de ERL

Los Operadores de ERL serán personal designado al efecto y autorizados por el personal del grupo DIVOPER/PKI.

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 DEFENSA-EC-WPG2016.
- 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.

6.2.1.6. Auditor

Puede acceder a cualquier elemento de PKIDEF y ver (en modo solo leer) los parámetros de la PKI, así como los ficheros de logs (trazas) generadas y los certificados emitidos.

6.2.1.7. 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 PKIDEF.

La realización de las copias de seguridad de los datos de operación es responsabilidad de la Subunidad de Servicios de Seguridad de Infraestructura y S.O. Cliente del CESTIC.

6.2.1.8. 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 al menos dos personas para la activación de claves de los dispositivos criptográficos hardware (HSM) 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 del grupo DIVOPER/PKI. Cualquier operación sobre las entidades ha de ser autorizada previamente y por escrito señalando un responsable del grupo DIVOPER/PKI que ha de velar por la correcta operativa.

6.2.1.9. Identificación y autenticación para cada perfil

Para acceder a las herramientas de gestión de los elementos de PKIDEF (y de la EC Subordinada en particular), el usuario deberá presentar un certificado de autenticación emitido por la propia DEFENSA-EC-WPG2016 en tarjeta criptográfica (TEMD).

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

6.2.1.10. 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, servidores seguros y servicios web.
- 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 otro distinto al descrito, se presentará solicitud escrita y detallada ante el responsable del grupo DIVOPER/PKI, para analizar el perfil de certificado correspondiente y la viabilidad tecnológica en los sistemas definidos para su uso. Igualmente es potestad del responsable del grupo DIVOPER/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 CESTIC.

6.3. 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.

6.4. Procedimientos de Control de Seguridad

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

6.4.1. Tipos de eventos a registrar

En el momento de la instalación de la EC Subordinada 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 Subordinada 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 DEFENSA-EC-WPG2016, 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 DEFENSA-EC-WPG2016 en particular).
- Los avisos (warnings) y errores producidos en el procesado de una petición por parte de DEFENSA-EC-WPG2016. Asimismo, se registrarán los avisos (warnings) y errores producidos por mecanismos internos de DEFENSA-EC-WPG2016 (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.

6.4.2. 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 Subordinada y ER) deberá almacenarse protegida hasta que la información se consolide para su revisión.

6.4.3. 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 6.5.2* Periodo de retención para el archivo.

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.

6.4.4. Protección del registro de eventos

Las medidas de seguridad de los registros de eventos deben 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 de ACESIN.

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.

6.4.5. 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 de ACESIN.

6.4.6. 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. Los servicios de recogida de información de eventos deben estar disponibles al arrancar los servicios de certificación, así como durante una solicitud concreta: si los servicios de recogida de información de eventos no están disponibles, no se podrán procesar peticiones de certificación ni 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.

6.4.7. Notificación al causante del evento

No estipulado.

6.4.8. 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. El grupo DIVOPER/PKI es el encargado 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 del grupo DIVOPER/PKI, puede solicitar periódicamente 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.

Adicionalmente se ejecutan análisis de vulnerabilidades trimestrales y un pentesting anual sobre toda la infraestructura de PKIDEF, gestionando aquellas vulnerabilidades críticas (si las hubiera) en un plazo inferior a 48 horas.

6.5. Archivo de informaciones y registros

6.5.1. Tipos de información archivada

El archivado de información de la EGC estará detallado para establecer la validez de una firma y 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 DEFENSA-EC-WPG2016:
  - 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 procedimientos de uso de la TEMD"*).
- La documentación relativa a la autenticación de la identidad del Subscriptor (como se describe en la *sección 4.2.3* Autenticación de la identidad de un individuo)
- La documentación relativa a la recepción y aceptación de certificados -Documento de Aceptación- (como se describe en la *sección 5.4* Aceptación de Certificados).
- Los registros de eventos especificados en la *sección 6.4* Procedimientos de Control de Seguridad 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 el grupo DIVOPER/PKI almacena, en una localización segura, una copia completa del software de los componentes de PKIDEF, para recuperar los sistemas bajo los que se creó la información e inspeccionó.

A nivel físico, el grupo DIVOPER/PKI garantiza la existencia de un módulo HSM SafeNet Luna G5 y un módulo HSM Realsec Cryptosec LAN, ambos con la información criptográfica específica, que permitan la recuperación del sistema PKIDEF.

6.5.2. Periodo de retención para el archivo

La información y documentación sobre el ciclo de vida de los certificados emitidos por PKIDEF se conservará durante 15 años una vez superada la fecha de validez de este (en total, 17 años).

6.5.3. 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 Subunidad de Servicios de Seguridad de Infraestructura y S.O. Cliente, aplicando las medidas estipuladas para el acceso y control.

6.5.4. Procedimientos de backup del archivo

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

6.5.5. 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.

6.5.6. Sistema de recogida de información de auditoría (interno vs externo)

El sistema de recogida de información es interno a PKIDEF.

6.5.7. Procedimientos para obtener y verificar información archivada

Solo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para verificar 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 solo se da en las plataformas autorizadas para ello del grupo DIVOPER/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. Si quiere recuperar información que exceda el tiempo de vida de la EC vigente, se reconstruirá el sistema de PKI correspondiente a la EC no vigente al momento de inspeccionar la información, procediendo a la recuperación del sistema e inspeccionando la información con el rol correspondiente, según la acción que se quiera realizar sobre dicha información.

6.6. 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, DEFENSA-EC-WPG2016 podrá emitir certificados durante los 9 primeros años de validez. Desde entonces, se generarán nuevos 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 esta son los mismos que para proporcionar la clave pública en vigor. En consecuencia, la nueva clave se publicará en DICODEF (ver *sección 3.1*).

6.7. Recuperación en Caso de Compromiso de una Clave o de Desastre

6.7.1. 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 esta.

En el caso de detectar un incidente de seguridad de alto impacto se notificará en un plazo menor de 24 horas al Organo Supervisor (Ministerio de Asuntos Económicos y Transformación Digital).

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

6.7.2. La clave pública de una Entidad se revoca

En caso de revocar el 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 generará, certificará 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 la EC Subordinada (DEFENSA-EC-WPG2016), se procederá a las siguientes acciones:

- Levantamiento de la EC Raíz, procediendo a la revocación de la EC Subordinada y publicación de la ARL correspondiente.

- Después, DEFENSA-EC-RAIZ emitirá un nuevo certificado para la EC Subordinada (DEFENSA-EC-WPG20xx), que se publicará en los repositorios de información corporativos.
- El certificado revocado de la entidad permanecerá accesible en DICODEF para verificar 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.

6.7.3. La clave de una Entidad se compromete

En el caso de compromiso de la clave de la EC Subordinada (DEFENSA-EC-WPG2016), 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 eliminarán los mismos de los repositorios por los mecanismos implementados en el sistema, y si fuera necesario, con los mecanismos propios de eliminación de DICODEF y Directorio Activo.
- Publicación de la CRL correspondiente.
- Levantamiento de la EC Raíz, procediendo a la revocación de la EC y publicación de la ARL correspondiente.
- Después, se generará 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 DEFENSA-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.

6.7.4. Recuperación en caso de desastre

Los sistemas de la PKI del Ministerio de Defensa se implementan en condiciones de alta disponibilidad y redundancia en todos 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 caso de indisponibilidad de las instalaciones de la Entidad de Certificación DEFENSA-EC-WPG2016 por más de veinticuatro horas, esta DPC remite al uso del Plan de Contingencia del CESTIC vigente.

6.8. 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* *6.7.2* La clave pública de una Entidad se revoca *y* *6.7.3* La clave de una Entidad se compromete de esta DPC.
- Decisión organizativa por parte del Ministerio de Defensa.

En caso de cese de su actividad como Prestador de Servicios de Confianza, 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 estos revocándolos.
- Comunicar al Ministerio competente en Sociedad de la Información y firma electrónica el cese de su actividad y el destino que dará a los certificados y 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.

7. 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.

7.1. Generación e Instalación del Par de Claves

7.1.1. Generación del par de claves

Las claves de la EC Raíz se generan y custodian en un módulo criptográfico SafeNet Luna G5, dispositivo certificado FIPS 140-2 nivel 3.

Las claves de la EC Subordinada (DEFENSA-EC-WPG2016) se generan y custodian en módulos criptográficos Realsec Cryptosec LAN, siendo estos dispositivos criptográficos certificados FIPS 140-2 alcanzando globalmente el nivel 3. Adicionalmente los módulos Realsec Cryptosec LAN poseen la certificación Common Criteria (CC) con nivel EAL4+ (ALC_FLR.1).

Las claves de las Entidades de Validación, Sellado de Tiempo y Entidades de Registro son generadas y custodiadas en los módulos Realsec Cryptosec LAN.

La generación de las claves de los certificados de usuarios en tarjeta, perfil de autenticación y firma, tiene lugar en la propia tarjeta TEMD, aceptada para su uso en el Ministerio de Defensa. La tarjeta TEMD dispone de estos modelos físicos:

- TEMDv1, fabricada por Microelectrónica Española (MEE), y diseñada originalmente con requisitos de seguridad equivalentes a una certificación CC EAL4+.
- TEMDv2, fabricada por la Fábrica Nacional de Moneda y Timbre (FNMT-RCM), y de nombre comercial TC- FNMT, que está siendo evaluada según los requisitos de la norma Common Criteria.
  - Cumple estrictamente el paquete de garantía EAL4+ con AVA_VAN.5.
  - Cumple estrictamente el perfil de protección “Protection profiles for Secure signature creation device — Part 2: Device with key generation” de CEN / CENELEC (TC224/WG17).
- TEMDv3, fabricada por la Fábrica Nacional de Moneda y Timbre (FNMT-RCM) basada en la anterior TEMDv2 con la incorporación un chip inalámbrico con tecnología DESFIRE EV2, que cubre todas las necesidades del Ministerio en cuanto a seguridad, capacidad y operatividad.

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 HSM.

En general, cuando el subscriptor es un dispositivo o sistema, 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 recomendable generar el certificado utilizando los algoritmos o longitudes de claves especificados en la ETSI TS 119 312. Es obligación del Agente de la PKI el custodiar de forma segura las claves generadas. Posteriormente, el envío de la solicitud de certificación a DEFENSA-EC-WPG2016 se hará en formato PKCS#10.

7.1.2. Entrega de la clave privada a los subscriptores

Ver la *sección 5.3.1* 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 autenticación y la de firma se generan en la tarjeta sin que sea extraída. La clave de cifrado se genera 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).

7.1.3. Entrega de la clave pública al emisor del certificado

Ver la *sección 5.1.2* 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.

7.1.4. 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 5.3.3* Distribución de la clave pública de la EC a los usuarios de PKIDEF.

Por otra parte, los terceros aceptantes podrán descargar los certificados confiables desde los repositorios identificados en la *sección 3.1*.

7.1.5. Longitud de las claves

La longitud de las claves RSA es 4096 bits para la EC Raíz (DEFENSA-EC-RAIZ), EC Subordinada (DEFENSA-EC-WPG2016) y EST (DEFENSA-EST-WPG2016).

La longitud de las claves RSA es 2048 bits para la EV (DEFENSA-EV-WPG2016), ER (DEFENSA-ER03-WPG2016 y DEFENSA-ER04-WPG2016).

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 2048 bits para los certificados en software de dispositivo (incluida Sede Electrónica de Nivel Medio) y de sistema (incluido Sello Electrónico de Nivel Medio).

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

7.1.6. 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**[5].

7.1.7. Comprobación de la calidad de los parámetros

La calidad de los parámetros en el módulo criptográfico SafeNet Luna G5 de la EC Raíz (DEFENSA-EC-RAIZ) es garantizada por la certificación FIPS 140-2 nivel 3.

La calidad de los parámetros en los módulos criptográficos Realsec Cryptosec LAN de la EC Subordinada, ER, EV y EST es garantizada por la acreditación FIPS 140-2 nivel 3.

La calidad de los parámetros en la Tarjeta TEMDv1, con tecnología de Microelectrónica, es garantizada por el cumplimiento de un nivel de seguridad equivalente a CC EAL4+. La calidad de los parámetros en la Tarjeta TEMDv2 y TEMDv3, con tecnología de FNMT-RCM, es garantizada por el cumplimiento estricto de un nivel de garantía CC EAL4+.

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

7.1.8. 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.

Las tarjetas criptográficas TEMD utilizadas para almacenar los certificados personales cumplen un nivel de seguridad CC EAL4+ o equivalente, según el modelo. 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.

7.1.9. 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, smartCardLogon	Uso de clave Restricciones básicas
FIRMA PERSONA (PERSONA FÍSICA / EMPLEADO PÚBLICO)	contentCommitment	emailProtection	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 contentCommitment keyEncipherment	clientAuth, emailProtection	Uso de clave Restricciones básicas
AUTENTICACIÓN WEB	digitalSignature KeyEncipherment	serverAuth	Uso de clave

			Restricciones básicas
DISPOSITIVO SEGURO	digitalSignature KeyEncipherment	serverAuth, ipSecUser, ipSecEndSystme	Uso de clave Restricciones básicas
CONTROLADOR DE DOMINIO	digitalSignature KeyEncipherment	clientAuth, serverAuth, keyPurposeKdc, smartCardLogon	Uso de clave Restricciones básicas
IDENTIFICACIÓN DISPOSITIVO	digitalSignature keyEncipherment keyAgreement	clientAuth	Uso de clave Restricciones básicas
FIRMA SISTEMA	digitalSignature contentCommitment keyEncipherment	clientAuth, emailProtection	Uso de clave Restricciones básicas
IDENTIFICACION SISTEMA	digitalSignature KeyEncipherment keyAgreement	clientAuth	Uso de clave Restricciones básicas
FIRMA DE CÓDIGO	digitalSignature contentCommitment	codeSigning	Uso de clave Restricciones básicas

Ilustración 9: Fines del uso de la clave

7.2. Protección de la Clave Privada

7.2.1. Estándares para los módulos criptográficos

El módulo SafeNet Luna G5 de la EC Raíz (DEFENSA-EC-RAIZ) cumple con la certificación FIPS 140-2 nivel 3.

Los módulos Realsec Cryptosec LAN del resto de entidades de la PKI (EC Subordinada, ER, EST y EV) cumplen con la certificación FIPS 140-2 nivel 3.

Las tarjetas criptográficas TEMD cumplen con un nivel de seguridad CC EAL4+ o equivalente, según el modelo.

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

7.2.2. 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.

Los certificados de dispositivo o sistema emitidos en software deben custodiarlos 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 (DEFENSA-EC-RAIZ, DEFENSA-EC-WPG2016, DEFENSA-ER03-WPG2016, DEFENSA-ER04-WPG2016, DEFENSA-EV-WPG2016 y DEFENSA-EST-WPG2016) 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 el grupo DIVOPER/PKI. El acceso y puesta en marcha del módulo SafeNet Luna G5 de la EC Raíz requiere la autenticación mediante token del Usuario de Seguridad del dispositivo, perteneciente también a el grupo DIVOPER/PKI. Para poder realizar estas acciones, el módulo ha de recuperarse previamente de la caja fuerte situada en las instalaciones seguras del grupo DIVOPER/PKI a través del Responsable del grupo DIVOPER/PKI.
- El acceso a cualquier clave privada de los módulos Realsec Cryptosec LAN que dan servicio a la EC Subordinada está protegido por un juego de tarjetas MasterKey (2 de 8) custodiado de manera personal e intransferible por al menos dos miembros del grupo DIVOPER/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.

7.2.3. 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 autenticación y de firma (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 del certificado de 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.

- Esta DPC solo permite recuperar (previa copia de seguridad y custodia de PKIDEF) las claves privadas de los certificados personales de cifrado (Persona Física y Empleado Público), para evitar pérdidas de información que ocasione 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 encuentra 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 el grupo DIVOPER/PKI.

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

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

Las claves privadas para los certificados de dispositivo o sistema generadas en software deberán custodiarse seguramente 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 (DEFENSA-EC-RAIZ, DEFENSA-EC-WPG2016, DEFENSA-ER03-WPG2016, DEFENSA-ER04-WPG2016, DEFENSA-EV-WPG2016 y DEFENSA-EST-WPG2016) 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 G54 tiene lugar en el grupo DIVOPER/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 el grupo DIVOPER/PKI a nivel lógico y CPD a nivel físico. El acceso requiere un proceso de autenticación múltiple basado en tarjeta en el paradigma de seguridad de los módulos criptográficos respectivos.

7.2.4. Copia de seguridad de la clave privada

Para la EC Raíz, en todo momento existe una copia de seguridad (cifrada) 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 (DEFENSA-EC-WPG2016, DEFENSA-ER03-WPG2016, DEFENSA-ER04-WPG2016, DEFENSA-EV-WPG2016 y DEFENSA-EST-WPG2016), en todo momento existe una copia de seguridad (cifrada) en soporte físico de las claves privadas. 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.

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.

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 estas a través del servicio de recuperación de claves, el cual es operado en exclusividad por el personal del grupo DIVOPER/PKI:

- El proceso de custodia de las claves privadas de los certificados personales de cifrado está 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 el grupo DIVOPER/PKI de forma específica a tal fin a través de su certificado de autenticación:

https://ec.mdef.es:9101/

La operativa con cualquier clave privada está restringida de manera única y exclusiva al personal del grupo DIVOPER/PKI designado, no permitiéndose la operativa de los sistemas que albergan a terceros.

7.2.5. 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 del grupo DIVOPER/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.

7.2.6. Introducción de la clave privada en el módulo criptográfico

La generación de las claves privadas de los componentes de PKIDEF siempre se da en los HSM, sin permitirse introducir material en los módulos distintos de la PKI o de la Plataforma de Servicios de Seguridad (PSSDEF) 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 Subordinada hasta resolución de la incidencia.

Para los certificados personales, la única clave que se introduce en las tarjetas TEMD es la correspondiente al certificado de cifrado, siendo las claves privadas de autenticación y de firma generadas de manera local en las tarjetas. La inclusión de material adicional criptográfico en las tarjetas está prohibida, salvo autorización de la AGPMD, y su detección provocará la revocación inmediata de los certificados y eliminación de dicha tarjeta mediante los sistemas de revocación de PKIDEF y gestión de tarjetas respectivamente.

7.2.7. Método de activación de la clave privada

En caso de certificados personales, el acceso a las claves privadas está protegido por PIN, que deberá conocerlo solo el propio subscriptor.

La clave privada tanto de DEFENSA-EC-RAIZ como de DEFENSA-EC-WPG2016 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 DEFENSA-EC-WPG2016 tiene lugar previa introducción del PIN de perfil Usuario del HSM, que se realizará siempre por un miembro del grupo DIVOPER/PKI. Además, la activación en el sistema de PKI se da mediante un proceso de autenticación (Política Básica) basado en tarjeta criptográfica bajo un protocolo de desafío respuesta.
- La activación de la clave privada de DEFENSA-EC-RAIZ, alojada en el HSM SafeNet Luna G5, tiene lugar previa introducción del PIN de activación que está en posesión del Responsable de Seguridad, a través del TSC del dispositivo. Además, la activación en el sistema de PKI se da mediante un proceso de autenticación múltiple (Política CWA) basado en tarjeta criptográfica bajo un protocolo de desafío respuesta.

7.2.8. 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.

7.2.9. Método de destrucción de la clave privada

En caso de proceder a la destrucción de una clave privada del módulo SafeNet Luna G5 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 Realsec Cryptosec LAN, se llevará a cabo a través de la herramienta de administración de Realsec, previa autenticación del operador de seguridad correspondiente.

Las claves serán borradas de los HSM 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 Administración, 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 la tarjeta criptográfica TEMD se procederá al reinicio del dispositivo, no procediéndose al borrado de los registros de seguridad de las claves de cifrados 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.

7.2.10. Clasificación de los Módulos Criptográficos

El Ministerio de Defensa (PKIDEF) realiza estudios de mercado y evaluaciones de los productos tanto software como hardware implantados en su infraestructura, utilizando en dichos estudios criterios abiertos y aceptados por el mercado.

7.3. Otros Aspectos de la Gestión del par de Claves

7.3.1. Archivo de la clave pública

Las claves públicas quedan almacenadas en los sistemas de archivado de PKIDEF, en el proceso de archivo de los certificados, un periodo de trece (13) años tras superar la fecha de validez de estas (en total, 15 años).

7.3.2. 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 dos (2) años, aunque al emitir DEFENSA-EC-WPG2016 puede establecer periodos inferiores.

El certificado de DEFENSA-EC-RAIZ tiene una validez de treinta y seis (36) años, el de DEFENSA-EC-WPG2016 de once (11) años, el de DEFENSA-EV-WPG2016 de un (1) año y el del resto de entidades de PKIDEF (ER y EST) de dos (2) años.

7.4. Datos de Activación

7.4.1. Generación y activación de los datos de activación

En caso de certificados personales, el acceso a las claves privadas está protegido por PIN, que deberá conocerlo solo 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 8 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 del grupo DIVOPER/PKI.

7.4.2. 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 de un módulo criptográfico, o token del Usuario de Seguridad del módulo SafeNet Luna G5.

En cuanto a los componentes físicos de activación de los HSM, éstos están sujetos a los mecanismos de seguridad disponibles en el grupo DIVOPER/PKI.

7.4.3. Otros aspectos de los datos de activación

No estipulado.

7.5. 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 del grupo DIVOPER/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 del grupo DIVOPER/PKI. Cualquier operativa física o lógica sobre dichas plataformas debe ser aprobada previamente por el Responsable del grupo DIVOPER/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 PKIDEF tiene lugar mediante un usuario específico definido a tal fin. El acceso de este usuario a los sistemas tiene lugar previa autenticación del personal del grupo DIVOPER/PKI, mediante usuario y contraseña de Directorio Activo de Windows, a través de los sistemas de acceso remoto seguro (Escritorio Remoto) en la red de gestión del Ministerio. El acceso a las plataformas no proporciona permisos de administrador o root.

Por otra parte, las aplicaciones informáticas de gestión de los servicios de PKIDEF (EC, ER, EST y EV) requieren la presentación de un usuario y contraseña específico para cada perfil de operación / administración. Cada acceso será almacenado en el registro de eventos de PKIDEF. Una vez autenticado, el usuario podrá realizar las operaciones permitidas a los roles que tenga asignados.

7.6. 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 de funciones de la EC, solo se podrán instalar aplicaciones o componentes de software relacionados 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.
- Igualmente, si es posible, los puestos de Operadores de ERL serán estaciones de trabajo dedicadas a esa labor y no se instalará software externo a la configuración identificada para realizar las funciones definidas para la ERL.

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.

7.7. 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. Además, existen y activan sistemas de seguridad adicionales que garantizan la detección de eventos potenciales que 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 del grupo DIVOPER/PKI.

7.8. Controles de Seguridad de los Módulos Criptográficos

Los requerimientos para los módulos criptográficos se describen en la *sección* *7.2.1* Estándares para los módulos criptográficos.

8. PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS (CRL)

8.1. Perfil de Certificado

8.1.1. Número de versión

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

8.1.2. 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 I del presente documento se recogen los perfiles de los certificados de entidad final que emite actualmente PKIDEF.

8.1.3. Identificadores de objeto (OID) de los algoritmos

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

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
dsa-with-sha256	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-sha2(3) 2}

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 certificará las claves públicas asociadas a los algoritmos criptográficos identificados anteriormente, y usará los de firma descritos antes para firmar certificados, listas de revocación de certificados y cualquier otro producto de PKIDEF.

8.1.4. 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.

8.1.5. 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”, organizationIdentifier “ORGANIZATION IDENTIFIER”, L “LOCALITY” 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=MINISTERIO DE DEFENSA, 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).

8.1.6. 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 2.2.*

8.1.7. Uso de la extensión “Policy Constraints”

No estipulado.

8.1.8. 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.
- **“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.

8.1.9. 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 con la RFC 5280.

8.2. Perfil de CRL

8.2.1. Número de versión

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

8.2.2. CRL y extensiones

8.2.2.1. ARL de la Entidad de Certificación Raíz (DEFENSA-CRL-EC-RAIZ)

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

Campo	Contenido	Critica
Versión	V2	
Signature		
AlgorithmIdentifier		
Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	

Campo	Contenido	Critica
IssuerName	CN = DEFENSA-EC-RAIZ, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES	
ThisUpdate	Fecha de emisión	
NextUpdate	90 días desde la fecha de emisión	
revokedCertificates		
userCertificate		
CertificateSerialNumber	Entero que indica al certificado que está siendo revocado	
RevocationDate	Fecha de revocación	
crlEntryExtension		NO
ReasonCode	No utilizado	
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	

Ilustración 10: ARL

8.2.2.2. CRL de la Entidad de Certificación Subordinada (DEFENSA-CRL-EC-WPG2016)

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

Campo	Contenido	Critica
Versión	V2	
Signature		
AlgorithmIdentifier		
Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	

Campo	Contenido	Critica
IssuerName	CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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		NO
ReasonCode	No utilizado	
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	

Ilustración 11: CRL

9. AUDITORÍA DE CONFORMIDAD

9.1. 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.

9.2. Identificación / cualificación del auditor

El auditor de seguridad deberá ser independiente, a nivel organizativo, de PKIDEF, y no deberá pertenecer en ningún caso al grupo DIVOPER/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.

9.3. 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 realizar sobre los módulos criptográficos HSM, estos los operará el personal del grupo DIVOPER/PKI, proporcionando 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 del grupo DIVOPER/PKI.

9.4. 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 a los requisitos establecidos en el Reglamento (UE) 910/2014, eIDAS.
- 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 DEFENSA-EC-RAIZ y DEFENSA-EC-WPG2016.

- 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 de este, 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 del grupo DIVOPER/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, junto con los aspectos críticos señalados, se auditará según las buenas prácticas definidas en ISO27001.

9.5. Acciones para 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* *9.6* Comunicación de resultados.
- El grupo DIVOPER/PKI propondrá las acciones correctivas para solucionar la deficiencia, indicando el tiempo estimado para su aplicación a la AGPMD.
- Una vez subsanada la deficiencia, habrá que hacer 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…

9.6. 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.

10. REQUISITOS COMERCIALES Y LEGALES

10.1. 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.

10.2. Capacidad financiera

El Ministerio de Defensa, como órgano central de la Administración General del Estado, no está obligada a constituir un seguro de responsabilidad civil, tal y como establece el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

10.3. Política de Confidencialidad

10.3.1. 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 el grupo DIVOPER/PKI la información criptográfica que conforma el acceso a la EC Raíz.
  - Se protege el acceso a las tarjetas Administración de los módulos criptográficos (HSM) 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 del grupo DIVOPER/PKI del Ministerio de Defensa, las contraseñas 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 sobre las operaciones de 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.

10.3.2. 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.

10.3.3. Responsabilidad para proteger información confidencial.

La comunicación de información confidencial relativa a la actividad del Prestador de Servicios de Confianza estará sujeta a la legislación vigente. La información relativa a la actividad en relación con la expedición y gestión de los Certificados podrá ser comunicada, en caso de requerimiento, como evidencia de certificación en caso de un procedimiento judicial, incluso sin consentimiento del Titular del Certificado, siempre que sea conforme a la legislación aplicable a esta materia.

10.3.4. 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.

10.4. Protección de datos personales

Toda información de carácter personal proporcionada a PKIDEF por los subscriptores de sus certificados será tratada de acuerdo con los términos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

La información personal de los certificados se obtiene del directorio corporativo del Ministerio de Defensa (DICODEF). Los datos requeridos serán los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios relacionados con la firma electrónica.
PKIDEF solo podrá comunicar informaciones sensibles o con datos personales en aquellos supuestos en los que así se le requiera por la autoridad pública competente y en los supuestos previstos legalmente.

10.4.1. Plan de privacidad

.El tratamiento de datos de carácter personal que realiza PKIDEF se alinea con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD), así como con los requisitos que sean de aplicación por normativa nacional específica en esta materia.

10.4.2. Información tratada como privada

La PKIDEF considera privada toda la información personal sobre las personas físicas usuarias de los Servicios de Confianza que no deba incorporarse a los certificados y en los mecanismos del Servicio de información y consulta sobre la validez de los certificados. En todo caso, es considerada información privada toda información personal recabada en los procesos de solicitud, renovación y revocación de certificados electrónicos (con la salvedad indicada en el siguiente apartado), las Claves Privadas que obrasen en poder del Prestador de Servicios de Confianza, así como toda aquella claramente identificada como tal.

La PKIDEF aplica las salvaguardas apropiadas para proteger la información privada.

10.4.3. Información no considerada privada

No se considera información privada aquella que se incorpora a los certificados electrónicos, la información relativa al estado de vigencia de estos, la fecha de inicio de dicho estado (activo, revocado, caducado…), así como el motivo que provocó el cambio de estado. Por tanto, los Certificados electrónicos, las Listas de Certificados Revocados y cualquier contenido de estos no es considerada información privada.

10.4.4. Responsabilidad para proteger la información privada

El Ministerio de Defensa garantiza el cumplimiento de sus obligaciones legales como prestador de servicios de confianza, según la Ley 6/2020, de 11 de noviembre, y según esto, y según los artículos 10 y 11 de dicha Ley, responderá por los daños y perjuicios causados en el ejercicio de la actividad propia.

10.4.5. Delegado de protección de datos

Véase “Política de privacidad” en el Portal PKI - Ministerio de Defensa (https://www.defensa.gob.es/pki/), donde se especifica que el Ministerio de Defensa, tal y como establece el nuevo Reglamento, tiene designado un Delegado de Protección de Datos (en adelante DPD). Los interesados podrán ponerse en contacto con el DPD a través de la siguiente dirección de correo electrónico: DPD@mde.esasdfasd fsdafasd fasdfasdsdfsdf

10.4.6. Registro de actividades de tratamiento

Véase “Política de privacidad” en el Portal PKI - Ministerio de Defensa (https://www.defensa.gob.es/pki/), donde se especifica que los datos personales recabados por el Ministerio de Defensa y sus diferentes organismos quedarán reflejados en el registro de actividades de tratamiento.

10.4.7. Derechos de los interesados

Véase "Política de privacidad" en el Portal PKI - Ministerio de Defensa (https://www.defensa.gob.es/pki/), donde se detallan los derechos de los interesados: acceder, rectificar, suprimir, delimitar el tratamiendo etc.

10.4.8. Notificación de violaciones de seguridad

Véase "Política de privacidad" en el Portal PKI - Ministerio de Defensa (https://www.defensa.gob.es/pki/).

10.4.9. Aviso y consentimiento para usar la información privada

La obtención de información privada de las personas físicas en los procesos ligados al ciclo de vida de los Certificados (solicitud, acreditación de la identidad, renovación, revocación…) se realizará, en cualquier caso, previa obtención del consentimiento de dichas personas de forma inequívoca, es decir, mediante una manifestación del interesado o mediante una clara acción afirmativa.

10.4.10. Divulgación conforme al proceso judicial o administrativo

La PKIDEF no divulgará datos personales, salvo petición por parte de las autoridades administrativas o judiciales.

10.5. 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.

10.6. Obligaciones y Responsabilidad Civil

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

10.6.1. Obligaciones de la Entidad de Certificación

La Entidad de Certificación Subordinada de la Red de Propósito General del Ministerio de Defensa (DEFENSA-EC-WPG2016) 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 Raíz y EC Subordinada, en los procesos de gestión del ciclo de vida de los certificados y control de las tarjetas, tienen las siguientes obligaciones:

- Realizar sus operaciones según esta DPC.
- Proteger sus claves privadas.

- Incorporan mecanismos de control de acceso basado en roles, que requieren, si así se exige, la autenticación simultánea múltiple de los operadores correspondientes.
  - En la EC Subordinada los grupos que requieren un proceso de autenticación múltiple son: Operadores de Recuperación de Claves, Operadores de Revocación de operadores de ERL y Operadores de Revocación Masiva.
  - Para los Operadores de Revocación Masiva se requiere que al menos uno de ellos no pertenezca al grupo DIVOPER/PKI, debiendo designarlo por la AGPMD. Si deberá proceder a dichas operaciones, la presencia del operador es obligada. El Responsable del grupo DIVOPER/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, una misma persona no puede disponer de dos roles distintos en el módulo criptográfico.
  - Los Operadores que operan la EC Subordinada necesitan de la participación de los roles que gestionan el módulo criptográfico. En este caso, es necesario que participen en la autenticación, al menos, dos personas con el mismo rol de módulo criptográfico para poder hacer las operaciones pertinentes.
- Discriminan roles específicos para la gestión y uso de los módulos criptográficos que soportan las claves privadas de las EC en la generación, custodia y destrucción segura de las claves.
  - El Usuario de Seguridad del SafeNet Luna G5, módulo criptográfico de la EC Raíz realiza la gestión de los tokens y del TSC para la puesta en marcha operativa del SafeNet Luna G5, 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 (en la tecnología Safelayer) ostente el cargo de Usuario de Seguridad del módulo SafeNet. Cada miembro del grupo DIVOPER/PKI custodia la llave que corresponde al rol con el que ha sido específicamente nombrado. En ningún caso se permitirá ninguna operación de la EC Raíz a personal civil o militar, que no sea miembro del grupo DIVOPER/PKI y esté asignado a tal fin.

  - La administración de los módulos criptográficos de la EC Subordinada y entidades asociadas se basa en división de roles a la que aplica los mismos criterios que los mencionados. En ningún caso se permite que un miembro del grupo DIVOPER/PKI sea simultáneamente Usuario de Seguridad del módulo SafeNet Luna G5 y custodio de las tarjetas de administración de los módulos Realsec Cryptosec LAN.
- 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.
- Hay que 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 digitales 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.
- Desasignar los privilegios a los operadores de ERL que estén haciendo un uso indebido de los mismos.
- Revocar los certificados en los términos de la *sección* 5.9 Suspensión y Revocación de Certificados y publicar los certificados revocados en la CRL en los servicios de directorio y servicio web referidos en la *sección 3.1*, con la frecuencia estipulada en la *sección* 5.9.3.1 Frecuencia de emisión de las CRL
  - PKIDEF revoca el certificado, eliminándolo de DICODEF y publicando inmediatamente la CRL actualizada, garantizando la consistencia de la información presente en DICODEF.
  - En caso de necesidad, hacer la revocación masiva de certificados por el personal asignado al grupo pertinente.
- Utilizar los servicios de repositorio que satisfagan las obligaciones reflejadas en la *sección 3.1.*

- Hay que asegurar que las obligaciones que se imponen a los subscriptores son las reflejadas en la *sección 10.6.3* Obligaciones de los subscriptores de la presente DPC, y que se les informará de las consecuencias del incumplimiento de estas.
- 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 https://www.defensa.gob.es/pki/dpc/
- Garantizar la disponibilidad de las CRL según lo dispuesto en la sección 5.9.4 Disponibilidad de un sistema en línea de verificación del estado de los certificados de esta DPC.
- Si la EC revoca un certificado, notificarlo a los usuarios de certificados según lo establecido en este documento y en la Política de Certificación.
- Operar de acuerdo con la legislación aplicable. En concreto con:
  - Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
  - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
  - 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.
- Proteger las claves bajo su custodia.
- No almacenar los datos de creación de firma, clave privada, de los subscriptores de certificados emitidos para usarse 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 Energía, Turismo y Agenda Digital, 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 la información y documentación relativa a un certificado digital y las declaraciones de prácticas vigentes durante quince años desde su expedición, para verificarse las firmas efectuadas con él.
- 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 de DIVOPER, 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 no se oponga a estas obligaciones estará sujeta a las acciones contempladas en la sección 9.5 Acciones a tomar por una deficiencia de esta DPC.

10.6.2. Obligaciones de la Entidad de Registro Local.

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

- Realizar sus operaciones según 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 emitir un certificado, a quien solicita sus servicios, de las obligaciones que asume, la forma que custodia los datos de creación de firma, el procedimiento para comunicar la pérdida o utilización indebida de dispositivos de creación y de verificación de firma, de las condiciones para usarlo y de la página web donde consultar 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 inmediatas, después de haber realizado 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 de este.
- 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.

10.6.2.1. 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 el grupo DIVOPER/PKI, previa autorización del Responsable del grupo DIVOPER/PKI y de la AGPMD.

Las ERL han de notificar al Responsable del grupo DIVOPER/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 del grupo DIVOPER/PKI.

Las máquinas que soporten las ERL son exclusivos, no debiéndose instalar software que no sea 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[6] que especifica la fecha de emisión. En ese momento el solicitante pasa a ser subscriptor, aceptando las prácticas de comportamiento y uso de los certificados descritos en esta 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 del grupo DIVOPER/PKI.

El Responsable del grupo DIVOPER/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 del grupo DIVOPER/PKI.

10.6.2.2. Particularidades de la ER.

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

Las máquinas desde las que se accede a las funcionalidades de administración de la ER se ubican exclusivamente en las instalaciones del grupo DIVOPER/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.

[6] *Ver Anexo VII.*

10.6.3. 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 contraseña 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.
- Se recomienda que el par de claves generados en la TEMD se utilice única y exclusivamente para firmas electrónicas.

10.6.4. 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 al realizar cualquier operación basada en ellos comprobando que el certificado es válido y no ha caducado o 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.
- Asumir la responsabilidad de verificar que la CA Subordinada encargada de emitir certificados cualificados del Proveedor de Servicios de Confianza se encuentra en la lista TSL. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de certificación (TSL, por sus siglas en inglés) de España, a través del enlace Sede electrónica del Ministerio de Asuntos Económicos y Transformación Digital - Lista de confianza de prestadores cualificados de servicios electrónicos de confianza (mineco.gob.es)
- 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 de este.

10.6.5. 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.

Además, el Ministerio de Defensa publica esta Declaración de Prácticas de Certificación mediante 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 esta.

10.7. Renuncias de garantías

PKIDEF puede rechazar todas las garantías del servicio que no se encuentren vinculadas a obligaciones establecidas por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, especialmente aquellas garantías de adaptación para un propósito particular del certificado.

10.8. 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 Confianza, cuando se incumplan las obligaciones que le impone la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, 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 revisa ni considera las restricciones en el certificado sobre sus posibles usos, o cuando no considere la suspensión o pérdida de vigencia del certificado publicado en la CRL, o cuando no verifique la firma electrónica.

10.9. Indemnizaciones

No estipulado.

10.10. Plazo y Finalización

No estipulado.

10.11. 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 2.5.* Las comunicaciones electrónicas se harán efectivas una vez que las reciba el destinatario al que van dirigidas.

Si se quiere solicitar un conjunto de certificados de pruebas, se contactará a través de la siguiente dirección de correo electrónico: seginfo-pki@mde.es.

10.12. 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.

10.12.1. 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 2.5*. Toda comunicación deberá incluir una descripción del cambio, su justificación y la información de la persona que solicita la modificación. La AGPMD, aceptará con modificaciones o rechazará los cambios propuestos tras haber completado su revisión. Todos los cambios en el documento deberán ser aprobados por la AGPMD.

Cuando se realicen modificaciones significativas en el presente documento, será publicado y difundido a todas las partes interesadas según lo especificado en la sección 10.12.2 Procedimientos de Publicación y Notificación.

10.12.2. 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 **https://defensa.gob.es/pki/dpc**

10.12.3. 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. Además, verifica que DEFENSA-EC-WPG2016 cumple con los requerimientos expresados en esta DPC para su operación.

10.13. 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.

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

10.14. 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:

- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- 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.

10.15. Conformidad con la Ley aplicable

La AGPMD declara que la presente DPC cumple con las prescripciones contenidas en la legislación aplicable reseñada en el apartado 10.14 anterior

10.16. Cláusulas Diversas

No estipulado.

10.17. Otras Cláusulas

No estipulado.

ANEXO I – PERFILES DE CERTIFICADOS

Todos los perfiles del Ministerio de Defensa se han adaptado a lo indicado en el nuevo reglamento Reglamento (UE) No 910/2014 (eIDAS) y más concretamente a los perfiles de certificados v2.0 de la AGE.

El Ministerio de Defensa ha obtenido la calificación de prestador de servicios de certificación que expide certificados cualificados tras haber superado una auditoría con éxito y conseguido la aprobación por el Ministerio de Energía, Turismo y Agenda Digital.

De este modo, se ha incorporado la extensión "Qualified Certificate Statements", y por tanto se consideran certificados cualificados, a aquellos certificados que han obtenido esa calificación.

CERTIFICADOS DE EMPLEADO PÚBLICO

10.17.1. Autenticación

Nombre del Perfil:	Certificado de Autenticación de Empleado Público
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.
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 39/2015.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***

Campo	Criticidad	Valor/Contenido
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Organizational Unit (OU)		OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.6.5. Serial Number		serialNumber = IDCES-00000000G
1.6.6. Surname		surname = DE LA CAMARA ESPAÑOL | 00000000G
1.6.7. Given Name		givenName = JUAN ANTONIO
1.6.8. Common Name (CN)		cn = DE LA CAMARA ESPAÑOL JUAN ANTONIO | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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
2.4. Extended Key Usage	NO	smartCardLogon, 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.mde.es/dpc/

Campo	Criticidad	Valor/Observaciones
2.5.2.2. User Notice		Notice Text= ”Certificado de empleado publico, nivel medio, autenticacion. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).”
2.5.3. Policy Identifier		OID 2.16.724.1.3.5.7.2
2.6. Subject Alternate Names	NO	
2.6.1. User Principal Name (UPN)		UPN = juandelaespa12@mdef.es ***OID 1.3.6.1.4.1.311.20.2.3***
2.6.2. Directory Name		
2.6.2.1. Tipo de certificado		Tipo = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO DE AUTENTICACION ***OID 2.16.724.1.3.5.7.2.1***
2.6.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = “MINISTERIO DE DEFENSA” ***OID 2.16.724.1.3.5.7.2.2***
2.6.2.3. NIF entidad suscriptora		NIF = “S2800231I” ***OID 2.16.724.1.3.5.7.2.3***
2.6.2.4. DNI/NIE del responsable		DNI = 00000000G ***OID 2.16.724.1.3.5.7.2.4***
2.6.2.5. Nombre de pila		N = “JUAN ANTONIO” ***OID 2.16.724.1.3.5.7.2.6***
2.6.2.6. Primer apellido		SN1 = “DE LA CAMARA” ***OID 2.16.724.1.3.5.7.2.7***
2.6.2.7. Segundo apellido		SN2 = “ESPAÑOL” ***OID 2.16.724.1.3.5.7.2.8***
2.6.2.8. Correo electrónico		“juanantonio.delacamara.espanol@mde.es” ***OID 2.16.724.1.3.5.7.2.9***
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***

Campo	Criticidad	Valor/Observaciones
2.9. cRLDistributionPoint	NO	
2.9.1. distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-calssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 12: Certificado de Autenticación de Empleado Público

10.17.2. Firma

Nombre del Perfil:	Certificado de Firma de Empleado Público
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.
Usos Permitidos:	Firma electrónica avanzada (según Reglamento eIDAS) 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 39/2015.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	SI.

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption

Campo	Criticidad	Valor/Contenido
		OID 1.2.840.113549.1.1.11
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Organizational Unit (OU)		OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.6.5. Serial Number		serialNumber = IDCES-00000000G
1.6.6. Surname		surname = DE LA CAMARA ESPAÑOL | 00000000G
1.6.7. Given Name		givenName = JUAN ANTONIO
1.6.8. Common Name (CN)		cn = DE LA CAMARA ESPAÑOL JUAN ANTONIO | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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	contentCommitment
2.4. Extended Key Usage	NO	emailProtection
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.3.12
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/

Campo	Criticidad	Valor/Observaciones
2.5.2.2. User Notice		Notice Text= "Certificado Cualificado de empleado publico, nivel medio, firma electronica. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.5.2.3. Policy Identifier		OID 0.4.0.194112.1.0
2.5.3. Policy Identifier		OID 2.16.724.1.3.5.7.2
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. QcType- esign		***OID 0.4.0.1862.1.6.1***
2.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
2.6.5. semanticsId-Natural		***0.4.0.194121.1.1***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.7.2. Directory Name		
2.7.2.1. Tipo de certificado		Tipo = CERTIFICADO DE FIRMA DE EMPLEADO PUBLICO DE NIVEL MEDIO ***OID 2.16.724.1.3.5.7.2.1***
2.7.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = "MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.7.2.2***
2.7.2.3. NIF entidad suscriptora		NIF = "S2800231I" ***OID 2.16.724.1.3.5.7.2.3***
2.7.2.4. DNI/NIE del responsable		DNI = 00000000G ***OID 2.16.724.1.3.5.7.2.4***
2.7.2.5. Nombre de pila		N = "JUAN ANTONIO" ***OID 2.16.724.1.3.5.7.2.6***
2.7.2.6. Primer apellido		SN1 = "DE LA CAMARA" ***OID 2.16.724.1.3.5.7.2.7***
2.7.2.7. Segundo apellido		SN2 = "ESPAÑOL" ***OID 2.16.724.1.3.5.7.2.8***
2.7.2.8. Correo electrónico		"juanantonio.delacamara.espanol@mde.es"

Campo	Criticidad	Valor/Observaciones
		OID 2.16.724.1.3.5.7.2.9
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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.10.2.distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.11. Authority Info Access	NO	
2.11.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2.Access Location		URI= http://ev.mde.es
2.11.3.Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 13: Certificado Cualificado de Firma de Empleado Público

10.17.3. Cifrado

Nombre del Perfil:	Certificado de Cifrado de Empleado Público
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.
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 solo se permite para transportar temporalmente información sensible, prohibiéndose su uso para custodiar y almacenar permanentemente cualquier tipo de información.*

	Mecanismo de cifrado del personal al servicio de las Administraciones Públicas según la Ley 39/2015.
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	SI
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Organizational Unit (OU)		OU = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO
1.6.5. Serial Number		serialNumber = IDCES-00000000G
1.6.6. Surname		surname = DE LA CAMARA ESPAÑOL | 00000000G
1.6.7. Given Name		givenName = JUAN ANTONIO
1.6.8. Common Name (CN)		cn = DE LA CAMARA ESPAÑOL JUAN ANTONIO | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits***

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 2.16.724.1.1.1.1.3.13
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= ”Certificado de empleado publico, nivel medio, cifrado. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).”
2.5.2.3. Policy Identifier		OID 2.16.724.1.3.5.7.2
2.6. Subject Alternate Names	NO	
2.6.1. rfc822Name		rfc822Name= juanantonio.delacamara.espanol@mde.es
2.6.2. Directory Name		
2.6.2.1. Tipo de certificado		Tipo = CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO DE NIVEL MEDIO PARA CIFRADO ***OID 2.16.724.1.3.5.7.2.1***
2.6.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = “MINISTERIO DE DEFENSA” ***OID 2.16.724.1.3.5.7.2.2***
2.6.2.3. NIF entidad suscriptora		NIF = “S2800231I” ***OID 2.16.724.1.3.5.7.2.3***
2.6.2.4. DNI/NIE del responsable		DNI = 00000000G ***OID 2.16.724.1.3.5.7.2.4***
2.6.2.5. Nombre de pila		N = “JUAN ANTONIO” ***OID 2.16.724.1.3.5.7.2.6***
2.6.2.6. Primer apellido		SN1 = “DE LA CAMARA” ***OID 2.16.724.1.3.5.7.2.7***
2.6.2.7. Segundo apellido		SN2 = “ESPAÑOL” ***OID 2.16.724.1.3.5.7.2.8***
2.6.2.8. Correo electrónico		“juanantonio.delacamara.espanol@mde.es”

Campo	Criticidad	Valor/Observaciones
		OID 2.16.724.1.3.5.7.2.9
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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2.Access Location		URI= http://ev.mde.es
2.10.3.Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 14: Certificado de Cifrado de Empleado Público

CERTIFICADOS DE PERSONA FÍSICA

10.17.1. 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 ser relevantes para el Ministerio de Defensa, bajo autorización de la AGPMD.
Registro:	Presencial.
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 Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Serial Number		serialNumber = IDCES-00000000G
1.6.5. Surname		surname = DE LA CAMARA ESPAÑOL | 00000000G
1.6.6. Given Name		givenName = JUAN ANTONIO
1.6.7. Common Name (CN)		cn = DE LA CAMARA ESPAÑOL JUAN ANTONIO | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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.***

Campo	Criticidad	Valor/Observaciones
2.3. Key Usage	SI	digitalSignature
2.4. Extended Key Usage	NO	smartCardLogon, 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.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado de persona fisica, nivel medio, autenticacion. 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. 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.		
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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 15: Certificado de Autenticación de Persona Física en TEMD

10.17.2. 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 ser relevantes para el Ministerio de Defensa, bajo autorización de la AGPMD.
Registro:	Presencial.
Usos Permitidos:	Firma electrónica avanzada (según Reglamento eIDAS) 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 Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Serial Number		serialNumber = IDCES-00000000G
1.6.5. Surname		surname = DE LA CAMARA ESPAÑOL | 00000000G
1.6.6. Given Name		givenName = JUAN ANTONIO

Campo	Criticidad	Valor/Contenido
1.6.7. Common Name (CN)		cn = DE LA CAMARA ESPAÑOL JUAN ANTONIO | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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	contentCommitment
2.4. Extended Key Usage	NO	emailProtection
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.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado de persona fisica, nivel medio, firma electronica. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.6.		
2.6.1.		
2.6.2.		
2.6.3.		
2.6.4.		
2.6.5.		
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

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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.10.2.distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.11. Authority Info Access	NO	
2.11.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2.Access Location		URI= http://ev.mde.es
2.11.3.Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 16: Certificado de Firma de Persona Física en TEMD

10.17.3. 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 ser relevantes para el Ministerio de Defensa, bajo autorización de la AGPMD.
Registro:	Presencial.
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 solo se permite para transportar temporalmente información sensible, prohibiéndose su uso para custodiar y almacenar permanentemente cualquier tipo de información.*
Publicación:	Rama PERSONAS de DICODEF
Custodia y Recuperación de Claves:	SI
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PERSONAS
1.6.4. Serial Number		serialNumber = IDCES-00000000G
1.6.5. Surname		surname = DE LA CAMARA ESPAÑOL | 00000000G
1.6.6. Given Name		givenName = JUAN ANTONIO
1.6.7. Common Name (CN)		cn = DE LA CAMARA ESPAÑOL JUAN ANTONIO | 00000000G
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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	keyEncipherment, dataEncipherment
2.4. Extended Key Usage	NO	emailProtection, clientAuth

Campo	Criticidad	Valor/Observaciones
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.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado de persona fisica, nivel medio, cifrado. 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= 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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 17: Certificado de Cifrado de Persona Física en TEMD

CERTIFICADOS DE SEDE ELECTRÓNICA

10.17.4. 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	12 meses
Suscriptores:	Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias en la relación con el ciudadano.
Registro:	Solicitud 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 39/2015. Adicionalmente permite vincular una sede electrónica con la persona física o jurídica titular del certificado.
Publicación:	SubRama SEDE ELECTRONICA, Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	SI

Campo	Criticidad	Valor/Contenido
3. X.509v1 Field		
3.1. Version		2 (= v3)
3.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
3.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
3.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
3.5. Validity		12 meses
3.5.1. Not Before		
3.5.2. Not After		
3.6. Subject		
3.6.1. Country (C)		C = ES
3.6.2. Locality (L)		L = MADRID
3.6.3. Organization (O)		O = UNIDAD ORGANIZATIVA
3.6.4. serialNumber		Sxxxxxxxx
3.6.5. organizationIdentifier		organizationIdentifier = VATES-Sxxxxxxxx
3.6.6. businessCategory		Government Entity
3.6.7. jurisdictionCountryName		ES
3.6.8. Common Name (CN)		CN= sede.defensa.gob.es

Campo	Criticidad	Valor/Contenido
3.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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 2.16.724.1.1.1.1.3.10
4.5.2. Policy Qualifier ID		
4.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
4.5.2.2. User Notice		Notice Text= ”Certificado cualificado de sede electronica, nivel alto. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).”
4.5.2.3. Policy Identifier		OID 0.4.0.194112.1.4
4.5.2.4. Policy Identifier		OID 2.16.724.1.3.5.5.1
4.5.2.5. Policy Identifier		OID 2.23.140.1.1
4.6. Qualified Certificate Statements	NO	
4.6.1. QcCompliance		***OID 0.4.0.1862.1.1***
4.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
4.6.3. QcType-web		***OID 0.4.0.1862.1.6.3***
4.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
4.6.5. semanticsId-Legal		***0.4.0.194121.1.2***
4.7. Subject Alternate Names	NO	
4.7.1.		

Campo	Criticidad	Valor/Observaciones
4.7.2. dnsName		dnsName= sede.defensa.gob.es
4.8. Issuer Alternative Name	NO	
4.8.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
4.8.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
4.9. basicConstraints	SI	
4.9.1. cA		FALSO
4.9.2. pathLenConstraint		***No utilizado***
4.10. cRLDistributionPoint	NO	
4.10.1.distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
4.10.2.distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
4.11. Authority Info Access	NO	
4.11.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
4.11.2.Access Location		URI= http://ev.mde.es
4.11.3.Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
4.11.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt
4.11.5.cabfOrganizationIdentifier (OID 2.23.140.3.1)	NO	(OID 2.23.140.3.1)
4.11.5.1.registrationSchemeIdentifier		registrationSchemeIdentifier = VAT
4.11.5.2.registrationCountry		registrationCountry = ES
4.11.5.3.registrationReference		registrationReference = NIF DEL ORGANISMO

Ilustración 18: Certificado Cualificado de Sede Electrónica de Nivel Alto

10.17.5. 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 2048 bits
Periodo de Validez	12meses
Suscriptores:	Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias en la relación con el ciudadano.

Registro:	Solicitud 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 39/2015. Adicionalmente permite vincular una sede electrónica con la persona física o jurídica titular del certificado.
Publicación:	SubRama SEDE ELECTRONICA, Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.5. Validity		12 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Locality (L)		L = MADRID
1.6.3. Organization (O)		O = UNIDAD ORGANIZATIVA
1.6.4. serialNumber		Sxxxxxxxx
1.6.5. organizationIdentifier		organizationIdentifier = VATES-Sxxxxxxxx
1.6.6. businessCategory		Government Entity
1.6.7. jurisdictionCountryName		ES
1.6.8. 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***

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.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= ”Certificado cualificado de sede electronica, nivel medio/sustancial. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).”
2.5.2.3. Policy Identifier		OID 0.4.0.194112.1.4
2.5.2.4. Policy Identifier		OID 2.16.724.1.3.5.5.2
2.5.2.5. Policy Identifier		OID 2.23.140.1.1
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. QcType-web		***OID 0.4.0.1862.1.6.3***
2.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
2.6.5. semanticsId-Legal		***0.4.0.194121.1.2***
2.7. Subject Alternate Names	NO	
2.7.1.		
2.7.2. dnsName		dnsName= sede.defensa.gob.es
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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.10.2.distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.11. Authority Info Access	NO	
2.11.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2.Access Location		URI= http://ev.mde.es
2.11.3.Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt
2.11.5.cabfOrganizationIdentifier (OID 2.23.140.3.1)	NO	(OID 2.23.140.3.1)
2.11.5.1.registrationSchemeIdentifier		registrationSchemeIdentifier = VAT
2.11.5.2.registrationCountry		registrationCountry = ES
2.11.5.3.registrationReference		registrationReference = NIF DEL ORGANISMO

Ilustración 19: Certificado Cualificado de Sede Electrónica de Nivel Medio

CERTIFICADOS DE SELLO ELECTRÓNICO

10.17.6. 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 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 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 39/2015.
Publicación:	SubRama SELLO ELECTRONICO, Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	SI

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = GENERICAS
1.6.4. Organizational Unit (OU)		OU = SELLO ELECTRONICO
1.6.5. Organizational Unit (OU)		OU = CESTIC
1.1.1. organizationIdentifier		organizationIdentifier = VATES-Sxxxxxxxx
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***

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	digitalSignature, contentCommitment, keyEncipherment
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.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= ”Certificado cualificado de sello electronico de Admon., organo o entidad de derecho publico, nivel medio. Expedido por el MINISDEFde España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).”
2.5.2.3. Policy Identifier		OID 0.4.0.194112.1.1
2.5.2.4. Policy Identifier		OID 2.16.724.1.3.5.6.2
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. QcType-eseal		***OID 0.4.0.1862.1.6.2***
2.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
2.6.5. semanticsId-Legal		***0.4.0.194121.1.2***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= sello@oc.mde.es
2.7.2. Directory Name		
2.7.2.1. Tipo de certificado		Tipo = “SELLO ELECTRONICO” ***OID 2.16.724.1.3.5.6.2.1***
2.7.2.2. Nombre de la entidad suscriptora		Entidad Suscriptora = “MINISTERIO DE DEFENSA” ***OID 2.16.724.1.3.5.6.2.2***
2.7.2.3. NIF entidad suscriptora		NIF = “Sxxxxxxxx” ***OID 2.16.724.1.3.5.6.2.3***

Campo	Criticidad	Valor/Observaciones
2.7.2.4. Denominación de sistema o componente		Denominación sistema = "SELLO SISTEMA AUTOMATIZADO DEL MINISTERIO DE DEFENSA" ***OID 2.16.724.1.3.5.6.2.5***
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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.10.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2. Access Location		URI= http://ev.mde.es
2.11.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 20: Certificado Cualificado de Sello Electrónico de Nivel Medio

CERTIFICADOS DE DISPOSITIVO

10.17.7. Autenticación Web

Nombre del Perfil:	Certificado de Autenticación Web del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.7
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	12 meses
Suscriptores:	Sitios web de la infraestructura del Ministerio de Defensa.
Registro:	Solicitud a través del responsable del servidor, que actúa como Agente de la PKI.
Usos Permitidos:	Permite la identificación segura de los sitios web 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. Adicionalmente permite vincular un sitio web con la persona física o jurídica titular del certificado.
Publicación:	Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	SI

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.5. Validity		12 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		
1.6.1. Country (C)		C = ES
1.6.2. Locality (L)		L = MADRID
1.6.3. Organization (O)		O = UNIDAD ORGANIZATIVA
1.6.4. SerialNumber		Sxxxxxxxx
1.6.5. organizationIdentifier		organizationIdentifier = VATES-Sxxxxxxxx
1.6.6. businessCategory		Government Entity
1.6.7. jurisdictionCountryName		ES
1.6.8. Common Name (CN)		CN = portal.mde.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits***

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	digitalSignature, keyEncipherment
2.4. Extended Key Usage	NO	serverAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.7
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado cualificado de autenticacion de sitios web, nivel medio/sustancial. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.5.3 Policy Identifier		OID 0.4.0.2042.1.4
2.5.4 Policy Identifier		OID 2.23.140.1.1
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. QcType-web		***OID 0.4.0.1862.1.6.3***
2.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
2.6.5. semanticsId-Legal		***0.4.0.194121.1.2***
2.7. Subject Alternate Names	NO	
2.7.1.		
2.7.2. dnsName		dnsName= portal.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	

Campo	Criticidad	Valor/Observaciones
2.9.1. cA		FALSO
2.9.2. pathLenConstraint		***No utilizado***
2.10. cRLDistributionPoint	NO	
2.10.1.distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.10.2.distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.11. Authority Info Access	NO	
2.11.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2.Access Location		URI= http://ev.mde.es
2.11.3.Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt
2.12 cabfOrganizationIdentifier (OID 2.23.140.3.1)	NO	(OID 2.23.140.3.1)
2.12.1 registrationSchemeIdentifier		registrationSchemeIdentifier = VAT
2.12.2 registrationCountry		registrationCountry = ES
2.12.3 registrationReference		registrationReference = NIF DEL ORGANISMO

Ilustración 21: Certificado Cualificado de Autenticación Web

10.17.8. Dispositivo Seguro

Nombre del Perfil:	Certificado de Dispositivo Seguro del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.5
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Estaciones de trabajo, firewalls, routers, cifradores en línea, servidores (bases de datos, FTP,…) y otros componentes de la infraestructura del Ministerio de Defensa.
Registro:	Solicitud a través del responsable del servidor o dispositivo, que actúa como Agente de la PKI.
Usos Permitidos:	Permite identificar los servidores y dispositivos de la infraestructura del Ministerio de Defensa y establecer comunicaciones seguras (incluyendo el cifrado del canal de los datos transmitidos), dotándolos de capacidades SSL/TLS e IPSEC.
Publicación:	Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
1.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.5. Common Name (CN)		CN = router.mdef.es CN = portal.mdef.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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	serverAuth, ipSecTunnel, ipSecUser, ipSecEndSystem
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.5

Campo	Criticidad	Valor/Observaciones
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado de dispositivo seguro, nivel medio/sustancial. 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= adminrouter@oc.mde.es rfc822Name= portalmde@oc.mde.es
2.6.2. dnsName		dnsName= router.mdef.es CN = portal.mdef.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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 22: Certificado de Dispositivo Seguro

10.17.9. Identificación de Dispositivo

Nombre del Perfil:	Certificado de Identificación de Dispositivo del Ministerio de Defensa

OID (Object Identifier):	2.16.724.1.1.1.1.2.16
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Estaciones de trabajo, servidores y otros componentes de la infraestructura del Ministerio de Defensa.
Registro:	Solicitud a través del responsable del controlador de dominio, que actúa como Agente de la PKI.
Usos Permitidos:	Permite la identificación del equipo como miembro de una red corporativa del Ministerio de Defensa. También puede ser usado para identificación de equipos en redes WIFI, usando EAP-TLS y Radius.
Publicación:	Rama DISPOSITIVOS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
1.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.5. Common Name (CN)		CN = dispositivo.mdef.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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, keyAgreement
2.4. Extended Key Usage	NO	clientAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.16
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= ”Certificado de identificacion de dispositivo, nivel medio/sustancial. 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= admindispositivo@oc.mde.es
2.6.2. dnsName		dnsName= dispositivo.mdef.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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***

Campo	Criticidad	Valor/Observaciones
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 23: Certificado de Identificación de Dispositivo

10.17.10. Controlador de Dominio

Nombre del Perfil:	Certificado de Controlador de Dominio del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.15
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Controladores de dominio de la infraestructura de Directorio Activo de Windows del Ministerio de Defensa.
Registro:	Solicitud 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 Subordinada 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 Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.5. Validity		24 meses
1.5.1. Not Before		
1.5.2. Not After		
1.6. Subject		

Campo	Criticidad	Valor/Contenido
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = DISPOSITIVOS
1.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.5. Common Name (CN)		CN = domaincontroller.mdef.es
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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, keyPurposeKdc, smartCardLogon
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.15
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= ”Certificado de controlador de dominio, nivel medio/sustancial. 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= admindc@oc.mde.es
2.6.2. dnsName		dnsName= domaincontroller.mdef.es
2.6.3. 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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt
2.11. Certificate Template Name		DomainController

Ilustración 24: Certificado de Controlador de Dominio

CERTIFICADOS DE SISTEMA O APLICACIÓN

10.17.11. Identificación Sistema

Nombre del Perfil:	Certificado de Identificación de Sistema para sistemas y aplicaciones del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.9
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	24 meses
Suscriptores:	Sistemas y aplicaciones del Ministerio de Defensa.
Registro:	Solicitud 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).
Publicación:	Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	NO

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = GENERICAS
1.6.4. Organizational Unit (OU)		OU = PSSDEF
1.6.5. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.6. Common Name (CN)		CN = Sistema MDEF
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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, keyAgreement
2.4. Extended Key Usage	NO	clientAuth
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.9

Campo	Criticidad	Valor/Observaciones
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado de identificacion de sistema, nivel medio/sustancial. 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= respsistema@oc.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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.10. Authority Info Access	NO	
2.10.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.10.2. Access Location		URI= http://ev.mde.es
2.10.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.10.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 25: Certificado de Identificación Sistema

10.17.12. Firma Sistema (Sello)

Nombre del Perfil:	Certificado de Firma Sistema (Sello) para sistemas y aplicaciones del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.8
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	24 meses

Suscriptores:	Sistemas y aplicaciones del Ministerio de Defensa.
Registro:	Solicitud 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 Cualificado:	SI

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = GENERICAS
1.6.4. Organizational Unit (OU)		OU = PSSDEF
1.6.5. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.6. Common Name (CN)		CN = Sistema MDEF
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits***

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	digitalSignature, contentCommitment, keyEncipherment
2.4. Extended Key Usage	NO	clientAuth, emailProtection
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.8
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= "Certificado cualificado de firma de sistema (sello electrónico), nivel medio/sustancial. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.5.2.3. policyIdentifier		OID 0.4.0.194112.1.1
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. QcType-eseal		***OID 0.4.0.1862.1.6.2***
2.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
2.6.5. semanticsId-Legal		***0.4.0.194121.1.2***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= respsistema@oc.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***

Campo	Criticidad	Valor/Observaciones
2.10. cRLDistributionPoint	NO	
2.10.1.distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.10.2.distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
2.11. Authority Info Access	NO	
2.11.1.Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2.Access Location		URI= http://ev.mde.es
2.11.3.Access Method		Access Method = Id-ad-calssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4.Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 26: Certificado Cualificado de Firma Sistema (Sello)

10.17.13. Firma de código

Nombre del Perfil:	Certificado de Firma de código del Ministerio de Defensa
OID (Object Identifier):	2.16.724.1.1.1.1.2.6
Soporte:	Software
Clave:	RSA 2048 bits
Periodo de Validez	No excederá de 38 meses
Suscriptores:	Sistemas y aplicaciones del Ministerio de Defensa.
Registro:	Solicitud a través del responsable del sistema o aplicación, que actúa como Agente de la PKI.
Usos Permitidos:	Garantiza la identidad del autor y la integridad del contenido de una aplicación software.
Publicación:	Rama GENERICAS de DICODEF
Custodia y Recuperación de Claves:	NO
Certificado Cualificado:	SI

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES

Campo	Criticidad	Valor/Contenido
1.5. Validity		No excederá de 38 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 = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PKI
1.1.2. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.4. Common Name (CN)		CN= DEFENSA-CODE-SIGNING 2016
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 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, contentCommitment
2.4. Extended Key Usage	NO	codeSigning
2.5. Certificate Policies	NO	
2.5.1. Policy Identifier		OID 2.16.724.1.1.1.1.2.6
2.5.2. Policy Qualifier ID		
2.5.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.5.2.2. User Notice		Notice Text= ”Certificado cualificado de firma de codigo, nivel medio/sustancial. Expedido por el Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).”
2.5.2.3. Policy Identifier		OID 0.4.0.194112.1.1
2.6. Qualified Certificate Statements	NO	
2.6.1. QcCompliance		***OID 0.4.0.1862.1.1***

Campo	Criticidad	Valor/Observaciones
2.6.2. QcEuRetentionPeriod		Integer:=15 ***OID 0.4.0.1862.1.3***
2.6.3. QcType-eseal		***OID 0.4.0.1862.1.6.2***
2.6.4. QcPDS		{https://pki.mde.es/pds/PDS_es.pdf, es}, {https://pki.mde.es/pds/PDS_en.pdf, en} ***OID 0.4.0.1862.1.5***
2.6.5. semanticsId-Legal		***0.4.0.194121.1.2***
2.7. Subject Alternate Names	NO	
2.7.1. rfc822Name		rfc822Name= pkiminisdef@oc.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		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
2.11. Authority Info Access	NO	
2.11.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
2.11.2. Access Location		URI= http://ev.mde.es
2.11.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
2.11.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 27: Certificado cualificado de Firma de código

ANEXO II – CERTIFICADOS DE LAS ENTIDADES DE CERTIFICACION DE PKIDEF

EC RAÍZ (DEFENSA-EC-RAIZ)

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-RAIZ, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.4.1. Country (C)		C = ES
1.4.2. Organization (O)		O = MINISTERIO DE DEFENSA
1.4.3. Organizational Unit (OU)		OU = PKI
1.4.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.4.5. Common Name (CN)		CN = DEFENSA-EC-RAIZ
1.5. Validity		36 años
1.5.1. Not Before		
1.5.2. Not After		viernes, 08 de noviembre de 2041 14:00:00
1.6. Subject		CN = DEFENSA-EC-RAIZ, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PKI
1.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.5. Common Name (CN)		CN = DEFENSA-EC-RAIZ
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 4096 bits***

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	keyCertSign, cRLSign
2.4. Certificate Policies	NO	
2.4.1. Policy Identifier		OID 2.5.29.32.0 (anyPolicy)
2.4.2. Policy Qualifier ID		
2.4.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.4.2.2. User Notice		Notice Text= "Certificado de la Entidad de Certificacion Raiz del Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid)."
2.5. Subject Alternate Names	NO	
2.5.1. rfc822Name		rfc822Name=agpmd@oc.mde.es
2.5.2. directoryName		directoryName= CN=Entidad de Certificacion Raiz, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
2.6. basicConstraints	SI	
2.6.1. cA		CIERTO
2.6.2. pathLenConstraint		***No utilizado***

Ilustración 28: Certificado DEFENSA-EC-RAIZ

EC SUBORDINADA (DEFENSA-EC-WPG2016)

Campo	Criticidad	Valor/Contenido
1. X.509v1 Field		
1.1. Version		2 (= v3)
1.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
1.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
1.4. Issuer Distinguished Name		CN = DEFENSA-EC-RAIZ, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.5. Validity		11 años
1.5.1. Not Before		

Campo	Criticidad	Valor/Contenido
1.5.2. Not After		
1.6. Subject		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
1.6.1. Country (C)		C = ES
1.6.2. Organization (O)		O = MINISTERIO DE DEFENSA
1.6.3. Organizational Unit (OU)		OU = PKI
1.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
1.6.5. Common Name (CN)		CN = DEFENSA-EC-WPG2016
1.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 4096 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	keyCertSign, cRLSign
2.4. Certificate Policies	NO	
2.4.1. Policy Identifier		OID 2.5.29.32.0 (anyPolicy)
2.4.2. Policy Qualifier ID		
2.4.2.1. CPS Pointer		http://pki.mde.es/dpc/
2.4.2.2. User Notice		Notice Text= Certificado de la Entidad de Certificacion Subordinada WPG2016 del Ministerio de Defensa de España (PKIDEF, CIF S2800231I, Arturo Soria 289 28071 Madrid).
2.5. Subject Alternate Names	NO	
2.5.1. rfc822Name		rfc822Name=agpmd@oc.mde.es
2.5.2. directoryName		directoryName= CN=Entidad de Certificacion Subordinada WPG2016, OU=Ministerio de Defensa de España, OU=PKI, O=MDEF, C=ES
2.6. basicConstraints	SI	

Campo	Criticidad	Valor/Observaciones
2.6.1. cA		CIERTO
2.6.2. pathLenConstraint		***0***
2.7. cRLDistributionPoint	NO	
2.7.1. distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-RAIZ.crl
2.7.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-RAIZ,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint

lustración 29: Certificado DEFENSA-EC-WPG2016

ANEXO III – CERTIFICADOS DE OTRAS ENTIDADES DE PKIDEF

ENTIDAD DE VALIDACIÓN (DEFENSA-EV-WPG2016)

Campo	Criticidad	Valor/Contenido
3. X.509v1 Field		
3.1. Version		2 (= v3)
3.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
3.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
3.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
3.5. Validity		6 meses
3.5.1. Not Before		
3.5.2. Not After		
3.6. Subject		CN = DEFENSA-EV-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
3.6.1. Country (C)		C = ES
3.6.2. Organization (O)		O = MINISTERIO DE DEFENSA
3.6.3. Organizational Unit (OU)		OU = PKI
3.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
3.6.5. Common Name (CN)		CN = DEFENSA-EV-WPG2016

Campo	Criticidad	Valor/Contenido
3.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits***

Campo	Criticidad	Valor/Observaciones
4. X.509v3 Extensions		-
4.1. OCSPNoCheck	NO	***1.3.6.1.5.5.7.48.1.5***
4.2. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
4.3. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
4.4. Key Usage	SI	digitalSignature
4.5. Extended Key Usage	NO	OCSPSigning
4.6. Certificate Policies	NO	
4.6.1. Policy Identifier		2.16.724.1.1.1.1.3.4
4.6.2. Policy Qualifier ID		
4.6.2.1. CPS Pointer		http://pki.mde.es/dpc/
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		FALSE
4.9. cRLDistributionPoint	NO	
4.9.1. distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
4.9.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
4.10. Authority Info Access	NO	
4.10.1. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
4.10.2. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 30: Certificado DEFENSA-EV-WPG2016

ENTIDAD DE SELLADO DE TIEMPO (DEFENSA-EST-WPG2016)

Campo	Criticidad	Valor/Contenido
5. X.509v1 Field		
5.1. Version		2 (= v3)
5.2. Serial Number		Establecido automáticamente por la Entidad de Certificación.
5.3. Signature Algorithm		sha256WithRSAEncryption ***OID 1.2.840.113549.1.1.11***
5.4. Issuer Distinguished Name		CN = DEFENSA-EC-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
5.5. Validity		5 años
5.5.1. Not Before		
5.5.2. Not After		
5.6. Subject		CN = DEFENSA-EST-WPG2016, organizationIdentifier = VATES-S2800231I, OU = PKI, O = MINISTERIO DE DEFENSA, C = ES
5.6.1. Country (C)		C = ES
5.6.2. Organization (O)		O = MINISTERIO DE DEFENSA
5.6.3. Organizational Unit (OU)		OU = PKI
5.6.4. organizationIdentifier		organizationIdentifier = VATES-S2800231I
5.6.5. Common Name (CN)		CN = DEFENSA-EST-WPG2016
5.7. Subject Public Key Info		RSAEncryption ***OID 1.2.840.113549.1.1.1*** ***Longitud de 2048 bits***

Campo	Criticidad	Valor/Observaciones
6. X.509v3 Extensions		-
6.1. Authority Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública de la EC emisora.***
6.2. Subject Key Identifier	NO	***Derivada de utilizar la función de hash SHA-1 sobre la clave pública del sujeto.***
6.3. Key Usage	SI	digitalSignature, contentCommitment, keyAgreement
6.4. Extended Key Usage	NO	timeStamping
6.5. Certificate Policies	NO	

Campo	Criticidad	Valor/Observaciones
6.5.1. Policy Identifier		2.16.724.1.1.1.1.3.4
6.5.2. Policy Identifier		2.16.724.1.1.1.2.2
6.5.3. Policy Qualifier ID		
6.5.3.1. CPS Pointer		http://pki.mde.es/dpc/
6.6. Issuer Alternative Name	NO	
6.6.1. rfc822Name		rfc822Name= agpmd@oc.mde.es
6.6.2. directoryName		directoryName= CN=PKIDEF, OU=Ministerio de Defensa de España, SerialNumber=S2800231I, L=Arturo Soria 289 28071 Madrid, OU=PKI, O=MDEF, C=ES
6.7. basicConstraints	SI	
6.7.1. cA		FALSE
6.8. cRLDistributionPoint	NO	
6.8.1. distributionPoint		URI= http://pki.mde.es/crl/DEFENSA-CRL-EC-WPG2016.crl
6.8.2. distributionPoint		URI= ldap://ldap.mde.es/cn=DEFENSA-CRL-EC-WPG2016,OU=PKI,O=MDEF,C=ES?certificateRevocationList?base?objectclass=cRLDistributionPoint
6.9. Authority Info Access	NO	
6.9.1. Access Method		Access Method = Id-ad-ocsp ***OID 1.3.6.1.5.5.7.48.1***
6.9.2. Access Location		URI= http://ev.mde.es
6.9.3. Access Method		Access Method = Id-ad-caIssuers ***OID 1.3.6.1.5.5.7.48.2***
6.9.4. Access Location		URI= http://pki.mde.es/ca/DEFENSA-EC-WPG2016.crt

Ilustración 31: Certificado DEFENSA-EST-WPG2016

ANEXO IV – 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 el grupo DIVOPER/PKI hayan asegurado la viabilidad tecnológica en el uso de los certificados.

Actualmente PKIDEF emite certificados electrónicos (cualificados y no cualificados) de:

- Persona Física: autenticación, firma electrónica, cifrado.
- Empleado Público según la Ley 39/2015: autenticación, firma electrónica, cifrado.
- Sede Electrónica y Sello Electrónico según la Ley 39/2015.
- Dispositivos: autenticación sitios web, dispositivos seguros e identificación dispositivos.
- Sistemas y aplicaciones: firma sistema (sello) e identificación sistema.
- Firma de Código.

Como norma general, **todas las aplicaciones y sistemas del Ministerio de Defensa (tanto de ámbito privado como público) 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 (a través del procedimiento de solicitud de alta correspondiente en SCANS).

La AGPMD podrá denegar la solicitud del servicio cuando considere que peligra la prestación del servicio de PKIDEF o su seguridad, porque se vaya en contra de las directrices expresadas en esta 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.

ANEXO V– PRESTACION DE LOS SERVICIOS DE VALIDACION 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 del grupo DIVOPER/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 CESTIC. Este tipo de incidencias deben ser resueltas en el ámbito de la AGPMD y el grupo DIVOPER/PKI del ACESIN.

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 VI– PERFILES DE CONFIANZA Y CRITERIOS DE SEGREGACION 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.	
Oficial de Seguridad	En todo momento hay al menos dos oficiales de seguridad distintos en las instalaciones de DICOPER.
Oficial de Registro	Existen en todo momento al menos dos oficiales de registro distintos en las instalaciones de DIVOPER
Oficial de Administración y Oficial de Recuperación	Existen en todo momento al menos dos oficiales de administración / Oficiales de Recuperación[7] distintos en las instalaciones de DIVOPER. Uno de ellos es el Responsable del grupo DIVOPER / PKI
Auditor Sistema	Existen en todo momento al menos dos auditores de administración distintos en las instalaciones de DIVOPER
Perfiles Operativos de la Gestión de los Módulos HSM de la Infraestructura de Clave Pública[8].	
Oficial Seguridad Primero HSM EC Raíz	Existen en todo momento al menos un Oficial de Seguridad Primero en las instalaciones de DIVOPER
Oficial Seguridad Segundo HSM EC Raíz.	Existen en todo momento al menos un Oficial de Seguridad Segundo en las instalaciones de DIVOPER
Perfil Usuario HSM EC Subordinada	Existen en todo momento al menos dos perfiles Usuario en las instalaciones de DIVOPER
Perfil Administrador HSM EC Subordinada	Existen en todo momento al menos dos perfiesl Administrador en las instalaciones de DIVOPER

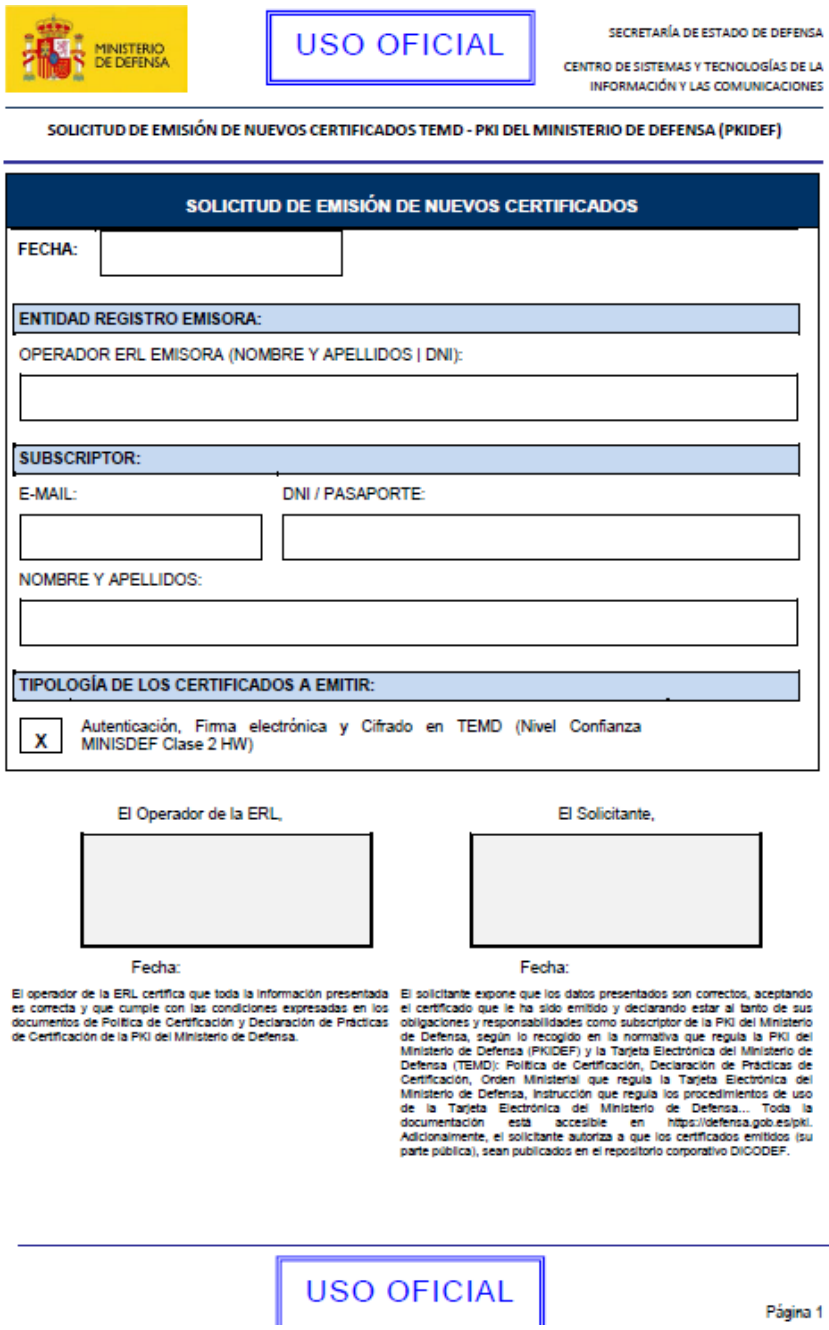
Ilustración 32: Perfiles de gestión del Ministerio de Defensa

7 El Responsable del Departamento tiene que tener asignado a este rol. Adicionalmente, 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 de DIVOPER.

8 No se permite en ningún caso que un miembro del grupo DIVOPER/PKI sea simultáneamente Oficial de Seguridad del módulo SafeNet y, simultánemente, custodio de las tarjetas de administración de los módulos Realsec.

ANEXO VII– PLANTILLAS DE USO EN LA ENTIDAD DE REGISTRO LOCAL

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



MINISTERIO DE DEFENSA

USO OFICIAL

SECRETARÍA DE ESTADO DE DEFENSA
CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

SOLICITUD DE EMISIÓN DE NUEVOS CERTIFICADOS TEMD - PKI DEL MINISTERIO DE DEFENSA (PKIDEF)

SOLICITUD DE EMISIÓN DE NUEVOS CERTIFICADOS

FECHA:

ENTIDAD REGISTRO EMISORA:

OPERADOR ERL EMISORA (NOMBRE Y APELLIDOS | DNI):

SUBSCRIPTOR:

E-MAIL:

DNI / PASAPORTE:

NOMBRE Y APELLIDOS:

TIPOLOGÍA DE LOS CERTIFICADOS A EMITIR:

X Autenticación, Firma electrónica y Cifrado en TEMD (Nivel Confianza MINISDEF Clase 2 HW)

El Operador de la ERL,

Fecha:

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

El Solicitante,

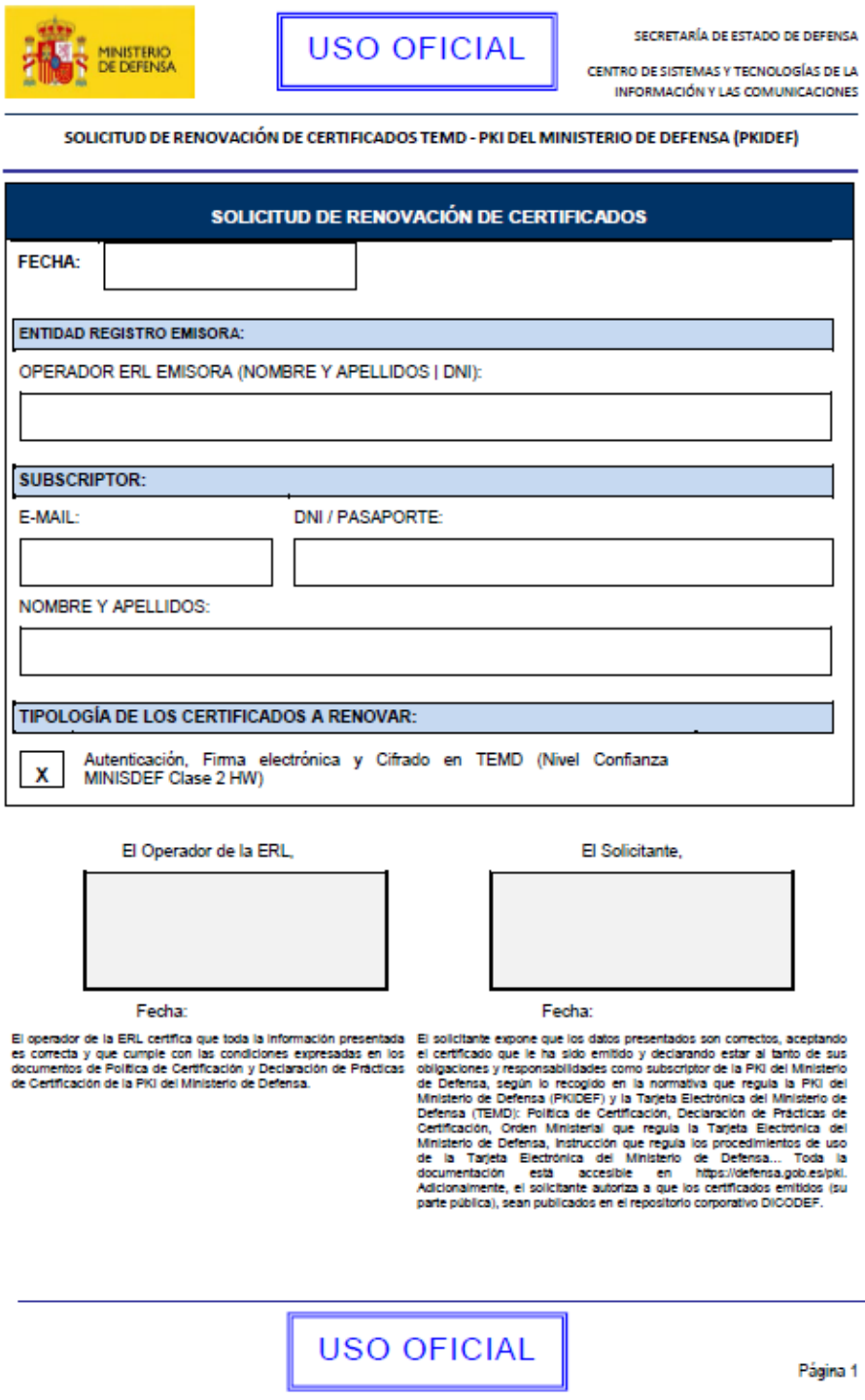
Fecha:

El solicitante expone que los datos presentados son correctos, aceptando el certificado que le ha sido emitido y declarando estar al tanto de sus obligaciones y responsabilidades como subscriptor de la PKI del Ministerio de Defensa, según lo recogido en la normativa que regula la PKI del Ministerio de Defensa (PKIDEF) y la Tarjeta Electrónica del Ministerio de Defensa (TEMD): Política de Certificación, Declaración de Prácticas de Certificación, Orden Ministerial que regula la Tarjeta Electrónica del Ministerio de Defensa, Instrucción que regula los procedimientos de uso de la Tarjeta Electrónica del Ministerio de Defensa... Toda la documentación está accesible en https://defensa.gob.es/pki. Adicionalmente, el solicitante autoriza a que los certificados emitidos (su parte pública), sean publicados en el repositorio corporativo DICODEF.

USO OFICIAL

Página 1

Ilustración 33: Plantilla de solicitud de emisión de certificados de la TEMD



MINISTERIO DE DEFENSA

USO OFICIAL

SECRETARÍA DE ESTADO DE DEFENSA

CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

SOLICITUD DE RENOVACIÓN DE CERTIFICADOS TEMD - PKI DEL MINISTERIO DE DEFENSA (PKIDEF)

SOLICITUD DE RENOVACIÓN DE CERTIFICADOS

FECHA:

ENTIDAD REGISTRO EMISORA:

OPERADOR ERL EMISORA (NOMBRE Y APELLIDOS | DNI):

SUBSCRIPTOR:

E-MAIL:

DNI / PASAPORTE:

NOMBRE Y APELLIDOS:

TIPOLOGÍA DE LOS CERTIFICADOS A RENOVAR:

[X] Autenticación, Firma electrónica y Cifrado en TEMD (Nivel Confianza MINISDEF Clase 2 HW)

El Operador de la ERL,

Fecha:

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

El Solicitante,

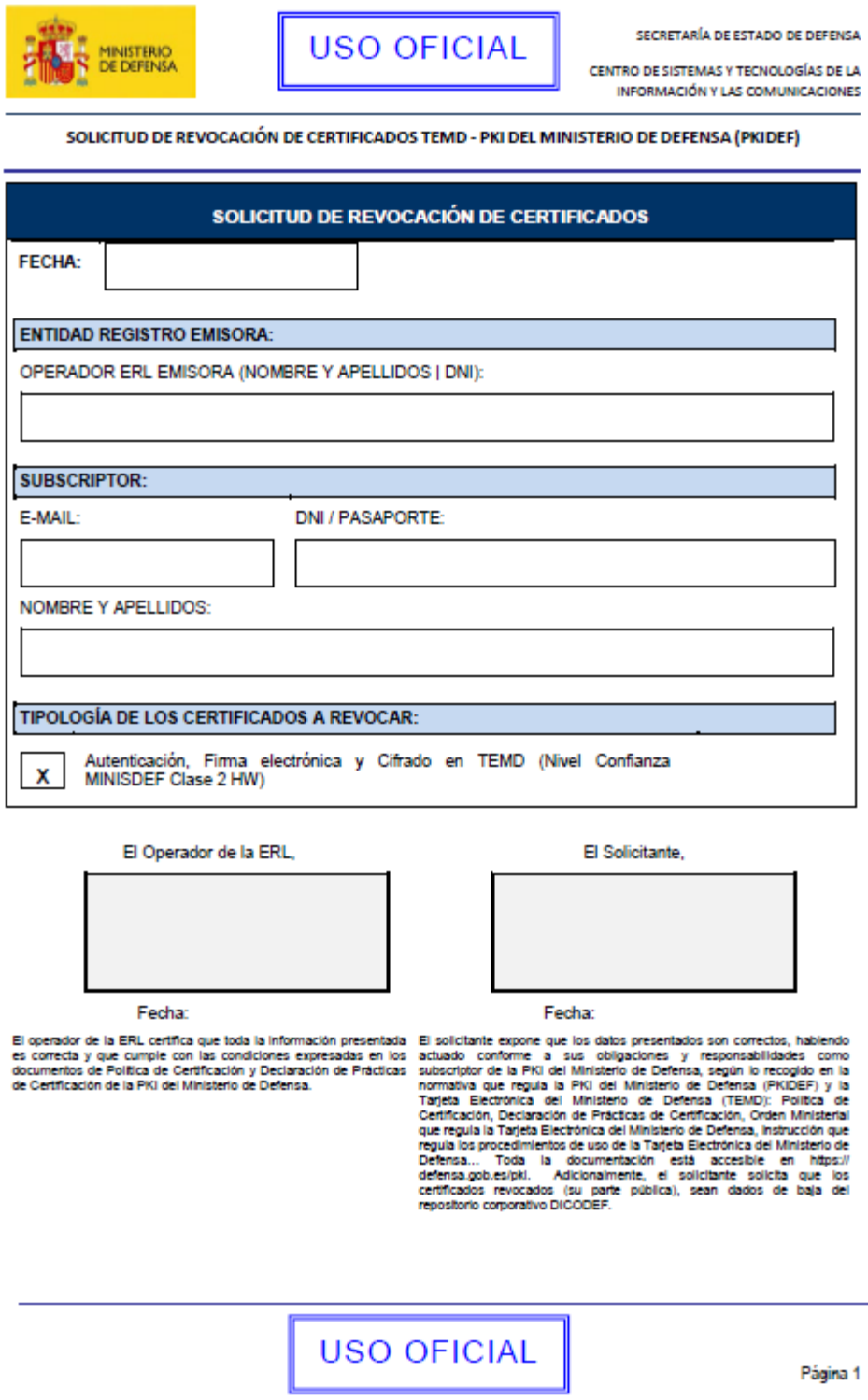
Fecha:

El solicitante expone que los datos presentados son correctos, aceptando el certificado que le ha sido emitido y declarando estar al tanto de sus obligaciones y responsabilidades como subscriptor de la PKI del Ministerio de Defensa, según lo recogido en la normativa que regula la PKI del Ministerio de Defensa (PKIDEF) y la Tarjeta Electrónica del Ministerio de Defensa (TEMD): Política de Certificación, Declaración de Prácticas de Certificación, Orden Ministerial que regula la Tarjeta Electrónica del Ministerio de Defensa, Instrucción que regula los procedimientos de uso de la Tarjeta Electrónica del Ministerio de Defensa... Toda la documentación está accesible en https://defensa.gob.es/pki. Adicionalmente, el solicitante autoriza a que los certificados emitidos (su parte pública), sean publicados en el repositorio corporativo DIRODEF.

USO OFICIAL

Página 1

Ilustración 34: Plantilla de solicitud de renovación de certificados de la TEMD



MINISTERIO DE DEFENSA

USO OFICIAL

SECRETARÍA DE ESTADO DE DEFENSA

CENTRO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

SOLICITUD DE REVOCACIÓN DE CERTIFICADOS TEMD - PKI DEL MINISTERIO DE DEFENSA (PKIDEF)

SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

FECHA:

ENTIDAD REGISTRO EMISORA:

OPERADOR ERL EMISORA (NOMBRE Y APELLIDOS | DNI):

SUBSCRIPTOR:

E-MAIL:

DNI / PASAPORTE:

NOMBRE Y APELLIDOS:

TIPOLOGÍA DE LOS CERTIFICADOS A REVOCAR:

[X] Autenticación, Firma electrónica y Cifrado en TEMD (Nivel Confianza MINISDEF Clase 2 HW)

El Operador de la ERL,

Fecha:

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

El Solicitante,

Fecha:

El solicitante expone que los datos presentados son correctos, habiendo actuado conforme a sus obligaciones y responsabilidades como subscriptor de la PKI del Ministerio de Defensa, según lo recogido en la normativa que regula la PKI del Ministerio de Defensa (PKIDEF) y la Tarjeta Electrónica del Ministerio de Defensa (TEMD): Política de Certificación, Declaración de Prácticas de Certificación, Orden Ministerial que regula la Tarjeta Electrónica del Ministerio de Defensa, Instrucción que regula los procedimientos de uso de la Tarjeta Electrónica del Ministerio de Defensa... Toda la documentación está accesible en https://defensa.gob.es/pki. Adicionalmente, el solicitante solicita que los certificados revocados (su parte pública), sean dados de baja del repositorio corporativo DICODEF.

USO OFICIAL

Página 1

Ilustración 35: Plantilla de solicitud de revocación de certificados de la TEMD

ANEXO VIII–MAPEO DE FUNCIONALIDADES DE LA RFC 3647 A LA PRESENTE DPC

RFC 3647	DPC PKIDEF
1.3 PKI participants	2.3 Comunidad y Ámbito de Aplicación
1.4.1 Appropiate Certiface Usage	2.4 Uso de los certificados
1.5.4 CPS Aproval procedures	2.5.3 Determinación de la aplicación de la DPC a la Política de Certificación
3.1.3 Anonymity or pseudonymity of subscribers	4.1.1 Tipos de nombre
3.2.4 Non-verified subscriber information	4.2.4 “Información no verificada del Subscriptor”:
3.2.5 Validation of authority	4.2.4 “Información no verificada del Subscriptor”
3.2.6 Criteria for interoperation	4.2.5 Criterios para Interoperación
4.2.1 Performing identification and authentication functions	5.1 Solicitud de certificados
4.2.2 Approval or rejection of certificate applications	5.1 Solicitud de certificados
4.2.3 Time to process certificate applications	Apartado 5.2.3 “Tramitación de la solicitud de los certificados”
4.4.1 Conduct constituting certificate acceptance	5.4 Aceptación de los certificados
4.6 Certificate Renewal	5.7 Renovación de Certificados con cambio de Claves (Renovación Simple)
4.6.7 Notification of certificate issuance by the CA to other entities	5.7.7 Notificación de la emisión del certificado por la CA a otras entidades
4.7 Certificate re-key 4.7.1 Circumstance for certificate re-key 4.7.2 Who may request certification of a new public key 4.7.3 Processing certificate re-keying requests 4.7.4 Notification of new certificate issuance to subscriber 4.7.5 Conduct constituting acceptance of a re-keyed certificate 4.7.6 Publication of the re-keyed certificate by the CA 4.7.7 Notification of certificate issuance by the CA to other entities	5.6 Renovación de Certificados sin cambio de Claves (Reemisión)
4.8 Certificate modification 4.8.1 Circumstance for certificate modification 4.8.2 Who may request certificate modification 4.8.3 Processing certificate modification requests 4.8.4 Notification of new certificate issuance to subscriber 4.8.5 Conduct constituting acceptance of modified certificate 4.8.6 Publication of the modified certificate by the CA 4.8.7 Notification of certificate issuance by the CA to other entities	5.8 Modificación de Certificados (Actualización)
4.9 Certificate revocation and suspensión	5.9 Suspensión y Revocación de Certificados
4.9.1 Circumstances for revocation	5.9.2.1 Circunstancias para la revocación
4.9.2 Who can request revocation	5.9.2.2 Quien puede solicitar la revocación
4.9.3 Procedure for revocation request	5.9.2.3 Procedimiento para la solicitud de revocación
4.9.4 Revocation request grace period	5.9.2.4 Periodo de gracia de la solicitud de revocación
4.9.5 Time within which CA must process the revocation request	5.9.2.5 Plazo en la ED debe resolver la solicitud de revocación

4.9.6 Revocation checking requirement for relying parties	5.9.5 Requisitos de verificación de las revocaciones por los Terceros Aceptantes
4.9.7 CRL issuance frequency (if applicable)	5.9.3.1 Frecuencia de emisión de las CRLs
4.9.8 Maximum latency for CRLs (if applicable)	5.9.3.2 Tiempo máximo entre la generación y la publicación de las CRL
4.9.9 On-line revocation/status checking availability	5.9.4 Disponibilidad de un sistema en línea de verificación del estado de los certificados
4.9.10 On-line revocation checking requirements	5.9.4.1 Requisitos de comprobación online de revocación
4.9.11 Other forms of revocation advertisements available	5.9.6 Otras formas de divulgación de información de revocaciones disponibles
4.9.12 Special requirements re key compromise	5.10, 5.9.2.3 y 10.6.3
4.9.13 Circumstances for suspensión	5.9.1 Suspensión
4.9.14 Who can request suspensión	5.9.1 Suspensión
4.9.15 Procedure for suspension request	5.9.1 Suspensión
4.9.16 Limits on suspension period	5.9.1 Suspensión
4.10 Certificate status services 4.10.1 Operational characteristics 4.10.2 Service availability 4.10.3 Optional features	5.10 Servicios de comprobación de estado de certificados
5.1.8 Off-site backup	6.1.8 Respaldo externo:
5.2 Procedural controls	6.2 Controles de Procedimiento
5.2.1 Trusted roles	6.2.1 Perfiles de confianza
5.2.2 Number of persons required per task	6.2.1.8 Número de personas requeridas por tarea
5.2.3 Identification and authentication for each role	6.2.1.9 Identificación y autenticación para cada perfil
5.2.4 Roles requiring separation of duties	6.2.1 Perfiles de Confianza
5.3 Personnel controls 5.3.1 Qualifications, experience, and clearance requirements 5.3.2 Background check procedures 5.3.3 Training requirements 5.3.4 Retraining frequency and requirements 5.3.5 Job rotation frequency and sequence 5.3.6 Sanctions for unauthorized actions 5.3.7 Independent contractor requirements 5.3.8 Documentation supplied to personnel	**6.3** Controles de Seguridad Personal
5.4 Audit logging procedures	6.4 Procedimientos de Control de Seguridad
5.7 Compromise and disaster recovery	6.7 Recuperación en Caso de Compromiso de una Clave o de Desastre
5.7.1 Incident and compromise handling procedures	6.7.1 Alteración de los recursos hardware, software y/o datos
5.7.2 Computing resources, software, and/or data are corrupted	6.7.1 Alteración de los recursos hardware, software y/o datos
5.7.3 Entity private key compromise procedures	6.7.2 La clave pública de una Entidad se revoca
5.7.4 Business continuity capabilities after a disaster	6.7.4 Recuperación en caso de desastre
6.2.11 Cryptographic Module Rating	7.2.10 Clasificación de los módulos criptográficos
6.5 Computer security controls	**7**.5 Controles de Seguridad Informática
6.5.1 Specific computer security technical requirements	7.5 Controles de Seguridad Informática
6.5.2 Computer security rating	7.6 Controles de Seguridad Informática
6.6 Life cycle technical controls	7.6 Controles de Seguridad del Ciclo de Vida
6.6.1 System development controls	7.6 Controles de Seguridad del Ciclo de Vida
6.6.2 Security management controls	7.6 Controles de Seguridad del Ciclo de Vida
6.6.3 Life cycle security controls	7.6 Controles de Seguridad del Ciclo de Vida
7.3 OCSP profile	Anexo IV

7.3.1 Version number(s) 7.3.2 OCSP extensions	
9.1 Fees 9.1.1 Certificate issuance or renewal fees 9.1.2 Certificate access fees 9.1.3 Revocation or status information access fees 9.1.4 Fees for other services 9.1.5 Refund policy 9.2 Financial responsibility 9.2.1 Insurance coverage 9.2.2 Other assets 9.2.3 Insurance or warranty coverage for end-entities	10.1 Tasas
9.3.3 Responsibility to protect confidential information	10.3.3 Responsabilidad para proteger información confidencial
9.4 Privacy of personal information 9.4.1 Privacy plan 9.4.2 Information treated as private 9.4.3 Information not deemed private 9.4.4 Responsibility to protect private information 9.4.5 Notice and consent to use private information 9.4.6 Disclosure pursuant to judicial or administrative process	Apartado 10.4 Véase el “Plan de Privacidad” en el Portal PKI - Ministerio de Defensa