DECLARACIÓN DE DIVULGACIÓN DE PKI (PDS)

CARNÉ PROFESIONAL, SEDE Y SELLO

DECLARACIÓN DE DIVULGACIÓN DE PKI (PDS)

TABLA DE CONTENIDOS

Pág.

1. DATOS DE CONTACTO DEL PRESTADOR 3
2. TIPOS DE CERTIFICADOS, PROCEDIMIENTOS DE VALIDACIÓN Y CONDICIONES DE USO 3
   2.1 TIPOS DE CERTIFICADOS 3
   2.2 PROCEDIMIENTOS DE VALIDACIÓN DE CERTIFICADOS 4
   2.3 CONDICIONES DE USO 5
      2.3.1 Usos apropiados de los certificados 5
      2.3.2 Limitaciones y restricciones en el uso de los certificados 8
3. OBLIGACIONES 9
   3.1 OBLIGACIONES DE LA AC 9
   3.2 OBLIGACIONES DE LA AR 10
   3.3 OBLIGACIONES DE LOS TITULARES DE LOS CERTIFICADOS 11
   3.4 OBLIGACIONES DE LOS TERCEROS ACEPTANTES 12
4. RESPONSABILIDADES 13
   4.1 LIMITACIONES DE RESPONSABILIDADES 13
   4.2 RESPONSABILIDADES DE LA AUTORIDAD DE CERTIFICACIÓN 13
   4.3 RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO 14
   4.4 RESPONSABILIDADES DEL TITULAR DE LOS CERTIFICADOS 14
   4.5 DELIMITACIÓN DE RESPONSABILIDADES 14
5. ACUERDOS APLICABLES Y DPC 15
6. POLÍTICA DE PRIVACIDAD 15
7. RECLAMACIONES Y JURISDICCIÓN 16
8. NORMATIVA APLICABLE 16
9. LICENCIAS, MARCAS REGISTRADAS Y AUDITORÍA 17
   9.1 LICENCIAS 17
   9.2 MARCAS REGISTRADAS 17
   9.3 AUDITORÍA 17

1. DATOS DE CONTACTO DEL PRESTADOR

Nombre	Dirección General de la Policía (Ministerio del Interior)		
Dirección e-mail	carnetprofesional@policia.es		
Dirección	C/Miguel Ángel 5 MADRID (España)		
Teléfono	+34913223400	**Fax**	+34913085774

2. TIPOS DE CERTIFICADOS, PROCEDIMIENTOS DE VALIDACIÓN Y CONDICIONES DE USO

2.1 TIPOS DE CERTIFICADOS

El servicio de expedición de certificados electrónicos cualificados de firma electrónica del Carné Profesional (empleado público con y sin seudónimo).

CERTIFICADO	KEY USAGE	EXTENDED KEY USAGE
Certificado de Firma (2.16.724.1.2.1.102.30 y 2.16.724.1.2.1.102.50)	contentCommitment[1]	
Certificado de Firma con seudónimo (2.16.724.1.2.1.102.41 y 2.16.724.1.2.1.102.51)	contentCommitment[2]	

Además, el Carné Profesional incorpora los siguientes tipos de certificados:

CERTIFICADO	KEY USAGE	EXTENDED KEY USAGE
Certificado de Autenticación (2.16.724.1.2.1.102.31 y 2.16.724.1.2.1.102.52)	Digital Signature	Autenticación del cliente Inicio de sesión de tarjeta inteligente Cualquier propósito Correo seguro
Certificado de Autenticación con seudónimo (2.16.724.1.2.1.102.60)	Digital Signature	Autenticación del cliente Correo seguro
Certificado de Cifrado (2.16.724.1.2.1.102.32 y 2.16.724.1.2.1.102.53)	Key Encipherment, Data Encipherment	Correo seguro Cualquier propósito Sistema de cifrado de archivos

El servicio de expedición de certificados electrónicos cualificados de sello electrónico.

[1] Nonrepudiation

CERTIFICADO	KEY USAGE	EXTENDED KEY USAGE
Certificado de Sello (niveles ALTO Y MEDIO) (2.16.724.1.2.1.102.36/37 y 2.16.724.1.2.1.102.57/58)	Digital Signature, Key Encipherment Content Commitment	Email Protection: Protección de mail Client Authentication: Autenticación de Cliente
Certificado de Sello electrónico para entidades externas a DGP (2.16.724.1.2.1.102.61/62)	Digital Signature, Key Encipherment Content Commitment	Email Protection: Protección de mail Client Authentication: Autenticación de Cliente

El servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web (sede electrónica).

CERTIFICADO	KEY USAGE	EXTENDED KEY USAGE
Certificado de Sede (niveles ALTO Y MEDIO) (2.16.724.1.2.1.102.34/35 y 2.16.724.1.2.1.102.55/56)	Digital Signature, Key Encipherment	Authentication TSL Web Server

2.2 PROCEDIMIENTOS DE VALIDACIÓN DE CERTIFICADOS

La(s) Autoridad(es) de Validación (AV) tienen como función la comprobación del estado de los certificados emitidos por las AC de la DGP, mediante el protocolo Online Certificate Status Protocol (OCSP), que determina el estado actual de un certificado electrónico a solicitud de un Tercero Aceptante sin requerir el acceso a listas de certificados revocados por éstas.

Este servicio de consulta debe prestarse tal y como establece la Ley 59/2003, de firma electrónica, en su artículo 18 apartado d: garantizando "*la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.*" y artículo 24 del Reglamento (UE) 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.

Dentro de la infraestructura de Clave Pública de la Dirección General de la Policía se ha desplegado una Autoridad de Validación para su uso interno por servicios propios de la Dirección General de la Policía. Dicha Autoridad de Validación cumple con los objetivos de universalidad y redundancia.

La información del estado de revocación se hará disponible más allá del periodo de validez del certificado durante el periodo de tiempo establecido por la normativa en vigor.
En este sentido, los certificados revocados que expiren serán retirados de la CRL, sin embargo se seguirá ofreciendo información del estado del certificado a través de la comprobación OCSP, independientemente de que esté caducado.
En el caso de compromiso de la clave privada de una Autoridad de Certificación o el cese de actividad del TSP, se proporcionará información del estado de revocación a través de los métodos/servicios de consulta habilitados al efecto conforme la DPC/PC.

Servicio de validación en línea que implementa el protocolo OCSP:

- WEB: http://ocsp.policia.es

El servicio de validación está disponible de forma ininterrumpida todos los días del año.

Por otro lado, la AC que emite las listas de CRLs emitirá una CRL indirecta completa que contendrá la identificación de todos los certificados revocados no caducados emitidos por la Infraestructura de Clave Pública de la DGP.

La validez de esta CRL estará establecida en 48 horas y será actualizada después de cada revocación o cada 23 horas (garantizándose así la disponibilidad de una nueva CRL antes de que se alcance la fecha indicada en el campo nextUpdate).

La ARL se ubicará en un archivo binario con nombre ARL.crl (http://www.policia.es/crls/ARL.crl y http://pki.policia.es/cnp/crls/ARL.crl).

La CRL completa se ubicará en un archivo binario con nombre CRL.crl (http://www.policia.es/crls/CRL.crl y http://pki.policia.es/cnp/crls/CRL.crl).

Asimismo, los certificados de entidad final incluyen como punto de distribución de CRL la URL http://www.policia.es/crls/CRL.crl o http://pki.policia.es/cnp/crls/CRL.crl.

2.3 CONDICIONES DE USO

2.3.1 Usos apropiados de los certificados

Los certificados emitidos por la Dirección General de la Policía serán utilizados para dar cumplimiento a las funciones que le son propias y legítimas, y para el desempeño de las funciones propias del personal al servicio de dicha Dirección General. Se emitirán como certificados cualificados de acuerdo con lo que se establece en los artículos 28, 38, 45 y anexos I, III, IV del Reglamento (UE) 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 así como en aquellos artículos de la Ley 59/2003, de 19 de diciembre, de firma electrónica que complementen, y se cumplirán las obligaciones determinadas en dichas Leyes y en las normativas específicas vigentes en el ámbito de la Administración General del Estado.

1. **Los Certificados de sede**, emitidos por la Dirección General de la Policía se utilizaran para la identificación de la sede electrónica y para el establecimiento de comunicaciones seguras con ellas. Por otro lado, el certificado de Sede electrónica (nivel MEDIO y ALTO) tiene en cuenta los requisitos de la política QCP-w según establece la norma europea EN 319 411-2.

   Asimismo, la Dirección General de la Policía se adhiere a las guías de requerimientos básicos para la emisión y gestión de certificados de confianza así como a las guías para la emisión y gestión de certificados de validación extendida, requisitos establecidos por la entidad CA/Browser forum. En caso de inconsistencia entre la DPC/PC y las guías, las últimas tendrán prioridad.

2. **Los Certificados de sello**, emitidos por la Dirección General de la Policía se utilizarán para garantizar la identificación y autenticación del ejercicio de las competencias del órgano o entidad titular en la actuación administrativa automatizada. Por otro lado, el certificado de Sello actuación automatizada tiene en cuenta los requisitos de la política QCP-l para el nivel MEDIO y QCP-l-qscd para el nivel ALTO según establece la norma europea EN 319 411-2.

3. **Los Certificados del Carné Profesional** (certificados de empleado público con y sin seudónimo), emitidos por la Dirección General de la Policía, se utilizaran para el desempeño de las funciones propias del personal al servicio de dicha Dirección General, tendrán como finalidad:

- **Certificado de Autenticación:** En su caso, garantizar electrónicamente la identidad del funcionario al realizar una transacción telemática. El Certificado de

Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá, a través de su certificado, acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen. Por tanto, los terceros aceptantes y los prestadores de servicios no tendrán garantía del compromiso del titular del Carné Profesional con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados cualificados por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

Este certificado lleva asociada a la identidad (nombre, apellidos y DNI/NIE) la capacidad profesional del titular, con la incorporación al certificado de la siguiente información adicional:

- Categoría profesional
- Dirección de correo corporativo
- Número de Carné profesional
- Identificador único del titular en los Sistemas de Información de la Dirección General de la Policía

Por otro lado, el certificado de autenticación del Carné Profesional (Empleado público con y sin seudónimo) nivel ALTO tiene en cuenta los requisitos de la política NCP+ según establece la norma europea EN 319 411-1.

- **Certificado de Firma:** El propósito de este certificado es permitir al funcionario firmar trámites o documentos. Este certificado (certificado cualificado según el Reglamento (UE) 910/2014) permite sustituir la firma manuscrita por la electrónica en las relaciones del titular del Carné Profesional con terceros (Artículo 25 del Reglamento (UE) 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).

El Reglamento (UE) 910/2014 establece que los certificados cualificados de firma electrónica cumplirán los requisitos establecidos en el anexo I. Por otro lado, la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

Los certificados de firma son certificados cualificados de acuerdo con lo que se establece en el artículo 28 y anexo I del Reglamento (UE) 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 así como en aquellos artículos de la Ley 59/2003, de 19 de diciembre, de firma electrónica que complementen.

Por otro lado, el certificado de firma del Carné Profesional (Empleado público con y sin seudónimo) nivel ALTO tiene en cuenta los requisitos de la política QCP-n-qscd según establece la norma europea EN 319 411-2.

Por lo anteriormente descrito, este certificado no deberá ser empleado para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

En su caso, este certificado lleva asociada a la identidad (nombre, apellidos y DNI/NIE) la siguiente información adicional:

- Categoría profesional
- Número de Carné profesional

- **Certificado de Cifrado:** Permitir el intercambio de información de manera segura, de tal manera que sólo el titular del certificado sea capaz de acceder a dicha información.

Los certificados de cifrado pueden utilizarse para prestar los siguientes servicios de seguridad:

- Cifrado de correos electrónicos
- Cifrado de ficheros
- Cifrado de transacciones

El uso del certificado de cifrado se limitará a ámbito profesional, quedando expresamente prohibido el uso personal del mismo; el titular del certificado debe ser consciente que la Dirección General de la Policía, almacena el material criptográfico asociado con el certificado de cifrado para su recuperación en caso de emergencia.

Este certificado lleva asociada a la identidad (nombre, apellidos y DNI/NIE) la siguiente información adicional:

- Categoría profesional
- Dirección de correo profesional
- Número de Carné profesional

4. **Los Certificados de sello para entidades externas a la DGP,** emitidos por la Dirección General de la Policía a órganos, organismos o entidades públicas externas a DGP así como entidades privadas externas a DGP se utilizarán con propósito único y exclusivo para trámites con la DGP en la realización de operaciones contra sus servicios no pudiéndose hacer uso del mismo en ningún otro servicio externo por parte de las entidades titulares de los certificados. Por otro lado, el certificado de Sello para entidades externas a la DGP tiene en cuenta los requisitos de la política QCP-l según establece la norma europea EN 319 411-2.

El uso conjunto de los certificados anteriores proporciona las siguientes garantías:

- Autenticidad de origen

El Funcionario podrá, a través de su **Certificado de Autenticación**, en su caso, acreditar su identidad frente a cualquiera, demostrando la posesión y el acceso a la clave privada asociada a la pública que se incluye en el certificado que acredita su identidad. Ambos clave privada y certificado, se encuentran almacenados en el Carné Profesional, el cual dispone de un procesador con capacidades criptográficas. Esto permite garantizar que la clave privada del titular (punto en el que se basa la credibilidad de su identidad) no abandona en ningún momento el

soporte físico del Carné Profesional. De este modo el titular, en el momento de acreditar electrónicamente su identidad, deberá estar en posesión de su Carné Profesional y de la clave personal de acceso (PIN) a la clave privada del certificado.

- No repudio de origen

Asegura que el documento proviene del titular de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del **Certificado de Firma**. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando el servicio de validación ofrecido por la Dirección General de la Policía. De esta forma se garantiza que el documento proviene de un determinado funcionario.

Dado que el Carné Profesional (empleado público con y sin seudónimo) niveles ALTO utilizan un dispositivo cualificado de creación de firma electrónica y que las claves de firma permanecen desde el momento de su creación bajo el control del titular, se garantiza el compromiso del mismo con la firma realizada (garantía de "no repudio").

- Integridad

Con el empleo del **Certificado de Firma**, se permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de su resumen.

- Confidencialidad

Mediante el uso del **Certificado de Cifrado** se garantiza que únicamente el destinatario del mensaje es capaz de acceder al contenido del mismo.

El emisor del mensaje, haciendo uso del certificado de cifrado del receptor, es capaz de cifrar la información contenida en dicho mensaje, de tal manera que sólo el receptor, en posesión de clave privada asociada al certificado, o personal autorizado actuando de oficio, sean capaces de acceder al contenido del mismo. Los procedimientos de archivo y recuperación de claves se describen en detalle en el apartado "4.12 Custodia y recuperación de claves" de la DPC.

El servicio encargado de la custodia y acceso a los certificados de cifrado y su clave privada asociada se denomina Servicio de Archivo y Recuperación de Claves descrito en la DPC.

2.3.2 Limitaciones y restricciones en el uso de los certificados

Los certificados emitidos por la Dirección General de la Policía deben emplearse únicamente de acuerdo con la legislación que le sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia de criptografía existentes en cada momento.

Los certificados no pueden utilizarse para actuar ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

Los usos de las claves de las Autoridades de Certificación se limita a la firma de certificados, generación de CRLs y OCSP.

Los certificados de Sede y de Sello no se utilizaran para fines distintos de los especificados en la presente Declaración de Practicas de Certificación.

Los certificados del Carné Profesional (empleado público con y sin seudónimo) podrán emplearse, en su caso, para autenticación (acreditación de identidad), firma electrónica (no repudio y compromiso con lo firmado) y confidencialidad (cifrado).

Tal y como se recoge en el apartado anterior el certificado de autenticación no deberá emplearse para la firma de trámites y documentos en los que se precisa dejar constancia del compromiso del firmante con el contenido firmado. Igualmente el certificado de firma no deberá ser empleado para firmar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

Los servicios de confianza que ofrece la Dirección General de la Policía, no han sido diseñados ni autorizados para ser utilizados en actividades de alto riesgo o que requieran una actividad a prueba de fallos, como las relativas al funcionamiento de instalaciones hospitalarias, nucleares, de control de tráfico aéreo o ferroviario, o cualquier otra donde un fallo pudiera conllevar la muerte, lesiones personales o daños graves al medioambiente.

El Carné Profesional (certificados de empleado público con y sin seudónimo) utilizan es un dispositivo cualificado de creación de firma electrónica y como tal, garantiza que las claves de firma y autenticación permanecen desde el momento de su creación bajo el control del titular y no es posible su exportación y uso desde cualquier otro dispositivo.

Respecto a la clave de cifrado, esta es generada externamente a la tarjeta, importada en la misma y custodiada adicionalmente por el Servicio de Archivo y Recuperación de Claves, de tal manera que pueda ser recuperada en el caso de que el titular, o persona autorizada, lo requiera.

El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de su carné profesional (certificados de Empleado público con y sin seudónimo) así como de los mecanismos de activación de las claves privadas, evitando su pérdida, divulgación, modificación o uso no autorizado.

3. OBLIGACIONES

3.1 OBLIGACIONES DE LA AC

La Autoridad de Certificación *Subordinada* actuará relacionando una determinada clave pública con su titular a través de la emisión de un certificado de firma cualificada, todo ello de conformidad con los términos de la Declaración de Prácticas y Políticas de Certificación (DPC).

Los servicios prestados por la AC en el contexto de la DPC son los servicios de emisión, renovación, suspensión y revocación de certificados cualificados y la provisión, en su caso, del dispositivo cualificado de creación de firma electrónica.

La AC tiene las siguientes obligaciones:

1º Realizar sus operaciones en conformidad con la DPC.

2º Publicar la DPC en el sitio web referido en el apartado 2.1 Repositorio.

3º Comunicar los cambios de la DPC de acuerdo con lo establecido en el apartado 9.12.2 Periodo y mecanismo de Notificación.

4º Cursar en línea la solicitud de un certificado y minimizar el tiempo necesario para expedir dicho certificado.

5º Emitir certificados que sean conformes con la información conocida en el momento de su emisión, y libres de errores de entrada de datos.

6º Revocar los certificados en los términos de la sección 4.4 Suspensión y Revocación de Certificados y publicar los certificados revocados en la CRL en el servicio de directorio y servicio Web referidos en el apartado 2.1 Repositorio, con la frecuencia estipulada en el punto 4.9.7 Frecuencia de emisión de CRLs de la DPC.

7º En el caso que la AC proceda de oficio a la revocación de un certificado, notificarlo a los usuarios de certificados en conformidad con la DPC.

8º Actualizar en línea y publicar las bases de datos de certificados en vigor y certificados revocados.

9º Poner a disposición de los funcionarios los certificados correspondientes a la(s) Autoridad(es) de Certificación de la Dirección General de la Policía (Ministerio del Interior).

10º Proteger la clave privada de la(s) Autoridad(es) de Certificación de la Dirección General de la Policía (Ministerio del Interior).

11º Conservar registrada toda la información y documentación relativa a los certificados emitidos por la Dirección General de la Policía durante un mínimo de quince años.

12º 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.

13º No almacenar en ningún caso los datos de creación de firma, clave privada, de los titulares de certificados del Carné Profesional, para los certificados de firma y autenticación.

14º Colaborar con los procesos de auditoría.

15º Operar de acuerdo con la legislación aplicable.

16º El prestador cualificado de servicio de confianza, Dirección General de la Policía (Ministerio del Interior), contará con un plan de cese actualizado para garantizar la continuidad del servicio, de conformidad con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17, apartado 4, letra i) tal como establece la letra i) del punto 2 artículo 24 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 el que se deroga la Directiva 1999/93/CE tal como se recoge en el epígrafe 5.8.1.

Así como todas las contempladas en el artículo 24 del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

3.2 OBLIGACIONES DE LA AR

Las Oficinas de Expedición de Certificados de la Dirección General de la Policía en su función de AR deberán cumplir las siguientes obligaciones:

1º Realizar sus operaciones en conformidad con la DPC.

2º Comprobar exhaustivamente la identidad de las personas.

3º Notificación de la emisión de los certificados al funcionario. No almacenando ni copiando los datos de creación de firma.

4º Tramitar las peticiones de revocación lo antes posible.

5º Notificación al funcionario de la revocación de sus certificados cuando se produzca de oficio por la Dirección General de la Policía (Ministerio del Interior), o a petición de la Autoridad competente en conformidad con la DPC.

6º Comprobar que toda la información incluida o incorporada por referencia en el certificado es exacta.

7º Respecto de la Protección de Datos de Carácter Personal, será de aplicación lo dispuesto en el apartado 10 de la DPC.

3.3 OBLIGACIONES DE LOS TITULARES DE LOS CERTIFICADOS

Es obligación de los titulares de los certificados emitidos bajo la DPC:

1º Suministrar a las Autoridades de Registro información exacta, completa y veraz con relación a los datos que estas les soliciten para realizar el proceso de registro.

2º Conocer y aceptar los términos y condiciones del servicio de confianza, en particular las contenidas en la DPC que le sean de aplicación, así como las modificaciones que se realicen sobre las mismas.

3º Comunicar a la Dirección General de la Policía, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento de los certificados o sus claves privadas.

4º Proteger sus claves privadas y custodiar los Certificados asociados, tomando las precauciones razonables para evitar su pérdida, revelación, alteración o uso no autorizado.

5º Aceptar las restricciones de uso establecidas en la DPC a las claves y certificados emitidos por la Dirección General de la Policía.

6º Solicitar inmediatamente la revocación de un certificado en caso de tener conocimiento o sospecha del compromiso de la clave privada correspondiente a la clave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros de la clave acceso y detección de inexactitudes en la información. La forma en que puede realizarse esta solicitud se encuentra especificada en el apartado 4.9.3.

7º No revelar la clave de acceso que permite la utilización de los certificados de la Dirección General de la Policía.

8º Informar inmediatamente a la Dirección General de la Policía acerca de cualquier situación que pueda afectar a la validez del Certificado.

9º Asegurarse de que toda la información contenida en el Certificado es correcta. Notificándolo inmediatamente en caso contrario.

10º No monitorizar, manipular o realizar actos de "ingeniería inversa" sobre la implantación técnica (hardware y software) de los servicios de certificación, sin permiso previo por escrito de la Autoridad de Confianza.

11º Cumplir las obligaciones que se establecen para el suscriptor este documento y en el artículo 23.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica así como el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

3.4 OBLIGACIONES DE LOS TERCEROS ACEPTANTES

A) Es obligación de los terceros que acepten y confíen en los certificados emitidos por la Dirección General de la Policía:

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y en la DPC.
- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos mediante la comprobación de que el certificado es válido y no está caducado o ha sido o revocado.
- Asumir su responsabilidad en la correcta verificación de las firmas electrónicas.
- Asumir su responsabilidad en la comprobación de la validez, revocación de los certificados en que confía.
- Conocer las garantías y responsabilidades derivadas de la aceptación de los certificados en los que confía y asumir sus obligaciones.
- Notificar cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo, utilizando los medios que la DGP publique en los sitios Web https://sede.policia.gob.es y www.policia.es

B) Los prestadores de servicios deberán verificar la validez de las firmas generadas por los certificados emitidos por la Dirección General de la Policía a través del Servicio de Validación de esta Dirección General.

- En el supuesto que no se realice dicha comprobación, la Dirección General de la Policía (Ministerio del Interior) no se hace responsable del uso y confianza que los prestadores de servicio otorguen a dichos certificados.
- En caso que el Prestador de Servicios consulte en línea el estado de un certificado (bien de sede, sello, autenticación, firma o cifrado) debe almacenar el comprobante de la transacción para tener derecho a realizar posteriores reclamaciones en caso que el estado del certificado en el momento de la consulta no coincida con su situación real.

C) Confianza en las firmas:

- El prestador de servicios debe adoptar las medidas necesarias para determinar la fiabilidad de la firma, construyendo toda la cadena de certificación y verificando la caducidad y el estado todos los certificados en dicha cadena.
- El prestador de servicios debe conocer e informarse sobre las Políticas y Prácticas de Certificación emitidos por la Dirección General de la Policía (Ministerio del Interior).
- Cuando se realice una operación que pueda ser considerada ilícita o se dé un uso no conforme a lo establecido en la DPC, no se deberá confiar en la firma emitida por el certificado.

D) Para confiar en los Certificados emitidos por la Dirección General de la Policía (Ministerio del Interior), el prestador de servicios deberá conocer y aceptar toda restricción a que esté sujeto el citado Certificado.

4. RESPONSABILIDADES

4.1 LIMITACIONES DE RESPONSABILIDADES

La Autoridad de Certificación de la Dirección General de la Policía responderá en el caso de incumplimiento de las obligaciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y normativa de desarrollo, en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza así como en la DPC.

En este sentido, el prestador de servicios de confianza asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.

4.2 RESPONSABILIDADES DE LA AUTORIDAD DE CERTIFICACIÓN

- La Dirección General de la Policía responderá por los daños y perjuicios que causen al firmante o terceros de buena fe cuando incumpla las obligaciones que impone la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 y la próxima Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.
- La responsabilidad del prestador de servicios de confianza regulada en la ley será exigible conforme a las normas generales sobre la culpa contractual o extra-contractual, según proceda, si bien corresponderá al prestador de servicios de confianza demostrar que actuó con la diligencia profesional que le es exigible siendo responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el Reglamento 910/2014.
- Se presumirá la intencionalidad o la negligencia de un prestador cualificado de servicios de confianza salvo cuando el prestador cualificado de servicios de confianza demuestre que los perjuicios a que se refiere el párrafo primero del artículo 13 del Reglamento 910/2014 se produjeron sin intención ni negligencia por su parte.
- Cuando DGP, como prestador cualificado de servicios de confianza, informe debidamente a los funcionarios con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero, el prestador de servicios de confianza no será responsable de los perjuicios producidos por una utilización de los servicios que vaya más allá de las limitaciones indicadas.
- De manera particular, la Dirección General de la Policía como prestador de servicios de confianza responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.
- La Dirección General de la Policía como prestador de servicios de certificación asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de confianza.
- La Dirección General de la Policía no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del funcionario y/o del prestador de servicio.

- La Dirección General de la Policía no será responsable de la utilización incorrecta de los Certificados ni de las claves, ni de cualquier daño indirecto que pueda resultar de la utilización de los Certificados.
- La Dirección General de la Policía no será responsable de los daños que puedan derivarse de aquellas operaciones en que se hayan incumplido las limitaciones de uso del Certificado.
- La Dirección General de la Policía no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones contenidas en la DPC si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia en la que no se pueda tener un control directo.
- La Dirección General de la Policía no será responsable del contenido de aquellos documentos firmados electrónicamente por los funcionarios con el Certificado de firma contenido en el Carné Profesional.
- La Dirección General de la Policía no garantiza los algoritmos criptográficos ni responderá de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si guardó la diligencia debida de acuerdo al estado actual de la técnica, y procedió conforme a lo dispuesto en la DPC y en la Ley.

4.3 RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO

La Autoridad de Registro asumirá toda la responsabilidad sobre la correcta identificación de los funcionarios y la validación de sus datos, con las mismas limitaciones que se establecen en el apartado anterior para la Autoridad de Certificación.

4.4 RESPONSABILIDADES DEL TITULAR DE LOS CERTIFICADOS

El titular de los certificados asumirá toda la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo informático o medio desde el cual emplee su certificado.

Así mismo el titular de los certificados se responsabilizará de los riesgos derivados de la aceptación de una conexión segura sin haber realizado previamente la preceptiva verificación de la validez del certificado exhibido por el prestador de servicios. Los procedimientos para contrastar la seguridad de la conexión con dicho prestador de servicios deberán ser proporcionados por éste al titular del certificado.

El Carné Profesional es un documento personal e intransferible emitido por la Dirección General de la Policía que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y es responsable de la conservación del mismo.

4.5 DELIMITACIÓN DE RESPONSABILIDADES

La Autoridad de Certificación de la Dirección General de la Policía no asume ninguna responsabilidad en caso de pérdida o perjuicio:

RESP.1	De los servicios que prestan, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
RESP.2	Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.

RESP.3	Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL
RESP.4	Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos y la DPC.
RESP.5	Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos.
RESP.6	Ocasionados por el mal uso de la información contenida en el certificado.
RESP.7	La AC no será responsable del contenido de aquellos documentos firmados electrónicamente ni de cualquier otra información que se autentiquen mediante un certificado emitido por ella.

5. ACUERDOS APLICABLES Y DPC

La Declaración y Políticas de certificación (dpc), los términos y condiciones del servicio de confianza así como la Declaración de divulgación de la PKI (pds) se encuentran publicados en las siguientes direcciones web:

Para la Declaración de Prácticas y Políticas de Certificación (DPC):

- WEB: http://www.policia.es/dpc y http://pki.policia.es/cnp/publicaciones/dpc

Para los términos y condiciones del servicio de confianza

- WEB: http://www.policia.es/terminos y http://pki.policia.es/cnp/publicaciones/terminos

Para la Declaración de divulgación de la PKI (PDS)

- WEB: https://www.policia.es/pds y https://pki.policia.es/cnp/publicaciones/pds

6. POLÍTICA DE PRIVACIDAD

De acuerdo con la legislación española en materia de protección de datos, se recoge dentro del capítulo 10 de la Declaración y Políticas de Certificación para dar cumplimiento a la dicha normativa.

Asimismo, la destrucción de un archivo de auditoría o registro solo se puede llevar a cabo con la autorización del Administrador del Sistema, el Responsable de Seguridad y el Administrador de Auditorías de la Infraestructura de Clave Pública de la Dirección General de la Policía. Tal destrucción se puede iniciar por la recomendación escrita de cualquiera de estas tres Autoridades o del administrador del servicio auditado, y siempre que hayan transcurrido los 15 años de retención.

Por último, tal como establece el artículo 24.2 h) 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, la Dirección General de la Policía (Ministerio del Interior) registrará y mantendrá accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos.

7. RECLAMACIONES Y JURISDICCIÓN

Todas reclamaciones entre usuarios y el prestador deberán ser comunicadas por la parte en disputa a la Autoridad de Aprobación de Políticas (AAP) de la Dirección General de la Policía (Ministerio del Interior), con el fin de intentar resolverlo entre las mismas partes.

Autoridad de Aprobación de Políticas (AAP) de la Infraestructura de Clave Pública de la Dirección General de la Policía.

Nombre	Grupo de trabajo de la Infraestructura de Clave Pública de la Dirección General de la Policía		
Dirección e-mail	carnetprofesional@policia.es		
Dirección	C/Miguel Ángel 5 MADRID (España)		
Teléfono	+34913223400	**Fax**	+34913085774

8. NORMATIVA APLICABLE

Las operaciones y funcionamiento de la Infraestructura de Clave Pública de la Dirección General de la Policía, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación que sean de aplicación para cada tipo de certificado, estarán sujetas a la normativa que les sea aplicable y en especial a:

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- 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 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- 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.
- Real Decreto 668/2015, de 17 de julio, por el que se modifica el 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 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).
- 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 951/2015, de 23 de octubre, de modificación del 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.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- ORDEN INT/761/2007, de 20 de marzo, por el que se aprueba el nuevo modelo de carné profesional de los funcionarios del Cuerpo Nacional de Policía y otros documentos identificativos.
- El Reglamento Orgánico y otras normas que afecten al funcionamiento de la Dirección General de la Policía.

9. LICENCIAS, MARCAS REGISTRADAS Y AUDITORÍA

9.1 LICENCIAS

En la actualidad, el prestador cualificado de servicios de confianza, Dirección General de la Policía, con CIF S2816015H se encuentra publicado en la lista de servicios de confianza accesible en https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

9.2 MARCAS REGISTRADAS

No estipulado.

9.3 AUDITORÍA

Se llevará a cabo una auditoría sobre el sistema de la infraestructura de Clave Pública de la Dirección General de la Policía de forma anual en conformidad con EN 319 411-2, de acuerdo con el Plan de Auditorías de la DGP. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en esta DPC.

Por otro lado, el Plan de Auditorías podrá contemplar el desarrollo de auditorías internas a las Autoridades de Registro en conformidad con EN 319 411-1 y el Reglamento 910/2014.

Sin perjuicio de lo anterior, que la DGP realizará auditorías internas bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

También, se establecerán controles periódicos en materia de protección de datos de carácter personal.

Por último, el prestador cualificado de servicios de confianza será auditado, al menos cada 24 meses por un organismo de evaluación de la conformidad según se establece en el Reglamento 910/2014.