DECLARACIÓN DE DIVULGACIÓN DE PKI (PDS)

DNI ELECTRÓNICO Y FIRMA CENTRALIZADA

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 3
   - 2.3 CONDICIONES DE USO 4
     - 2.3.1 Usos apropiados de los certificados 4
     - 2.3.2 Limitaciones y restricciones en el uso de los certificados 7
3. OBLIGACIONES 8
   - 3.1 OBLIGACIONES DE LA AC 8
   - 3.2 OBLIGACIONES DE LA AR 9
   - 3.3 OBLIGACIONES DE LOS CIUDADANOS TITULARES DE LOS CERTIFICADOS . 10
   - 3.4 OBLIGACIONES DE LOS TERCEROS ACEPTANTES 11
4. RESPONSABILIDADES 12
   - 4.1 LIMITACIONES DE RESPONSABILIDADES 12
   - 4.2 RESPONSABILIDADES DE LA AUTORIDAD DE CERTIFICACIÓN 12
   - 4.3 RESPONSABILIDADES DE LA AUTORIDAD DE REGISTRO 13
   - 4.4 RESPONSABILIDADES DEL CIUDADANO 13
   - 4.5 DELIMITACIÓN DE RESPONSABILIDADES 14
5. ACUERDOS APLICABLES Y DPC 14
6. POLÍTICA DE PRIVACIDAD 14
7. RECLAMACIONES Y JURISDICCIÓN 15
8. NORMATIVA APLICABLE 15
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	certificados@dnielectronico.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 DNI electrónico y certificados de firma centralizada de Ciudadano.

Certificado de Firma (2.16.724.1.2.2.2.3)	contentCommitment[1]
Certificado de Autenticación (2.16.724.1.2.2.2.4)	Digital Signature
Certificado de Firma Centralizada (2.16.724.1.2.2.2.11)	contentCommitment

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 para el DNI para ciudadanos españoles y extranjeros, 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.

El escenario inicial de segmentación de Autoridades de Validación (que cumple con los objetivos de universalidad y redundancia) es el siguiente:

- **Ministerio de Hacienda y Función Pública**, utilizará para las repuestas de validación (OCSP) del DNI, el certificado utilizado para la verificación de los Servicios de Firma electrónica e Identidad digital de la plataforma @firma.

[1] Nonrepudiation

- **Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda**, que prestaría sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.

La verificación de las revocaciones es obligatoria para cada uso de los certificados de identidad pública y firma electrónica. El procedimiento ordinario de comprobación de la validez de un certificado será la consulta a los Prestadores de Servicios de Validación, los cuales mediante protocolo OCSP indicarán el estado del certificado.

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 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.dnie.es

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

2.3 CONDICIONES DE USO

2.3.1 Usos apropiados de los certificados

Los Certificados de Identidad Pública y firma electrónica del Documento Nacional de Identidad (DNI), emitidos por la Dirección General de la Policía (Ministerio del Interior) tendrán como finalidad:

- **Certificado de Autenticación:** Garantizar electrónicamente la identidad del ciudadano 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 DNI 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.

  Asimismo, el documento nacional de identidad electrónico destaca por el cumplimiento con los requisitos de reconocimiento mutuo por parte de organismos del sector público de los Estados miembros a efectos de autenticación trasfronteriza del servicio prestado en línea por dichos organismos de acuerdo con el artículo 6 del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014. (DOUE 2018/C 401/08)

  Por otro lado, este certificado 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 ciudadano 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 ciudadano 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, este certificado tiene en cuenta los requisitos de la política QCP-n-qscd según establece la norma europea EN 319 411-2.

  Son certificados cualificados que se utilizan en dispositivo cualificado de creación de firma electrónica, de acuerdo con el artículo 29 y anexo II 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.

  Por este motivo, garantizan la identidad del ciudadano poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha estado generada utilizando un dispositivo cualificado de creación de firma electrónica, por lo cual, de acuerdo con lo que establece el 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, tendrá un efecto jurídico equivalente al de una firma manuscrita, sin necesidad de cumplir ningún otro requerimiento adicional.

  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).

  Dado que, técnicamente es posible la disociación de los certificados contenidos en el documento nacional de identidad electrónico, el Real Decreto 869/2013, de 8 de noviembre, introduce una modificación al decreto regulador del documento nacional de identidad (1553/2005), a fin de permitir que todos los ciudadanos españoles puedan acreditar su identidad por medios electrónicos, al tiempo que se reserva la capacidad de realizar la firma electrónica de documentos a las personas con capacidad legal para ello.

  Este Real Decreto establece que "en el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado".

  También se establece que "la activación del certificado de firma electrónica en el documento nacional de identidad tendrá carácter voluntario y su utilización se

realizará mediante una clave personal y secreta que el titular del documento nacional de identidad podrá introducir reservadamente en el sistema".

El uso conjunto de ambos certificados proporciona las siguientes garantías:

- Autenticidad de origen

  El Ciudadano podrá, a través de su **Certificado de Autenticación**, 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 Documento Nacional de Identidad, el cual dispone de un procesador con capacidades criptográficas. Esto permite garantizar que la clave privada del ciudadano (punto en el que se basa la credibilidad de su identidad) no abandona en ningún momento el soporte físico del Documento Nacional de Identidad. De este modo el ciudadano, en el momento de acreditar electrónicamente su identidad, deberá estar en posesión de su DNI y de la clave personal de acceso (PIN) a la clave privada del certificado.

- No repudio de origen

  Asegura que el documento proviene del ciudadano 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 cualquiera de los Prestadores de Servicios de Validación del DNI. De esta forma garantiza que el documento proviene de un determinado ciudadano.

  Dado que el DNI es 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 ciudadano 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.

Por otro lado, el Certificado de firma centralizada del Documento Nacional de Identidad emitido a ciudadanos españoles y extranjeros por la Dirección General de la Policía (Ministerio del Interior) tendrá como finalidad:

- **Certificado de firma centralizado:** El propósito de este certificado es permitir al ciudadano firmar trámites o documentos. Este certificado es un certificado cualificado según el Reglamento (UE) 910/2014.

  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, este certificado tiene en cuenta los requisitos de la política QCP-n según establece la norma europea EN 319 411-2.

El uso del certificado de firma proporciona las siguientes garantías:

- No repudio de origen

  Asegura que el documento proviene del ciudadano 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 cualquiera de los Prestadores de Servicios de Validación del certificado de firma centralizado. De esta forma garantiza que el documento proviene de un determinado ciudadano.

  Dado que en el sistema de firma con certificados centralizados se garantiza que las claves de firma permanecen, con un alto nivel de confianza, bajo el control del ciudadano titular, se garantiza el compromiso del mismo con la firma realizada (garantía de "no repudio").

- Integridad

  Con el empleo del Certificado de Firma Centralizado, 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.

2.3.2 Limitaciones y restricciones en el uso de los certificados

Los certificados 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 emitidos por la Dirección General de la Policía (Ministerio del Interior) solamente podrán emplearse para autenticación (acreditación de identidad) y para firmar electrónicamente (no repudio y compromiso con lo firmado), en caso del DNI.

El perfil de los certificados no contempla el uso de dichos certificados y sus claves asociadas para cifrar ningún tipo de información.

Los certificados no pueden utilizarse para actuar ni como Autoridad de Registro 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.

Asimismo, 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 DNI, 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 DNI es un dispositivo cualificado de creación de firma electrónica y como tal, garantiza que las claves permanecen desde el momento de su creación bajo el control del ciudadano titular del DNI y que no es posible su exportación y uso desde cualquier otro dispositivo. El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de su tarjeta así como de los mecanismos de activación de las claves privadas, evitando su pérdida, divulgación, modificación o uso no autorizado.

Por otro lado, se garantiza que las claves de firma permanecen, con un alto nivel de confianza, bajo el control del ciudadano titular del certificado de firma centralizada. El titular deberá poner el cuidado y medios necesarios para garantizar la custodia de las claves de acceso al certificado, evitando su pérdida, divulgación, modificación o uso no autorizado.

3. OBLIGACIONES

3.1 OBLIGACIONES DE LA AC

La Autoridad de Certificación *Subordinada* de DNI y de los certificados de firma centralizada 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 y revocación de certificados de firma cualificada personales y la provisión 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 10.12.2 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 ciudadanos 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 del DNI y de firma centralizada 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 ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se aplicarán los procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el firmante controle de modo exclusivo el uso de sus datos de creación de firma.

Solo los prestadores de servicios de confianza que expidan certificados cualificados podrán gestionar los datos de creación de firma electrónica en nombre del firmante. Para ello, podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No podrán duplicar los datos de creación de firma para ninguna otra finalidad.

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.

17º Cuando el prestador de servicios gestione los datos de creación de firma en nombre del firmante, deberá custodiarlos y protegerlos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante.

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 del DNI y de los certificados de firma centralizada 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 la pareja de certificados al ciudadano, en el caso de la expedición del DNI. No almacenando ni copiando los datos de creación de

firma de los certificados DNI o sin proteger siendo sólo accesibles por los titulares de los certificados de firma centralizada.

4º Tramitar las peticiones de revocación lo antes posible.

5º Notificación al ciudadano 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 11 de la DPC.

8º Poner a disposición de los ciudadanos, en las oficinas de expedición del DNI, los mecanismos adecuados para que pueda comprobar la veracidad de los datos.

9º Las obligaciones de las entidades registradores establecidas en la Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones, por las que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

3.3 OBLIGACIONES DE LOS CIUDADANOS 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 Conservar y utilizar de forma correcta el Documento Nacional de Identidad y los Certificados y claves. Su titular estará obligado a la custodia y conservación del mismo.

4º Comunicar a la Autoridad Competente, a través de los mecanismos que se habilitan a tal efecto, cualquier malfuncionamiento del certificado.

5º Proteger sus claves privadas, así como claves de acceso y custodiar los Certificados asociados, tomando las precauciones razonables para evitar su pérdida, revelación, alteración o uso no autorizado.

6º Aceptar las restricciones de uso (apartado 1.4.2 de la DPC) impuestas a sus claves y certificados emitidos por la Dirección General de la Policía (Ministerio del Interior).

7º 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 personal de 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 de la DPC.

8º No revelar la clave personal de acceso que permite la utilización de los certificados del DNI y de los certificados de firma centralizada.

9º Informar inmediatamente a la Autoridad Competente acerca de cualquier situación que pueda afectar a la validez del Certificado.

10º Asegurarse de que toda la información contenida en el Certificado y en el Documento Nacional de Identidad es correcta. Notificarlo inmediatamente en caso contrario.

11º No monitorizar, manipular o realizar actos de "ingeniería inversa" sobre la implantación técnica (hardware y software) de los servicios de confianza, sin permiso previo por escrito de la Autoridad de Certificación.

12º Cumplir las obligaciones que se establecen para los ciudadanos titulares de los certificados en 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 DNI y de firma centralizada:

- 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 Dirección General de la Policía (Ministerio del Interior) habilite a tal efecto.

B) Los prestadores de servicios deberán verificar la validez de las firmas generadas por los ciudadanos a través de la red de Prestadores de Servicios de Validación:

- 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 de DNI y de firma centralizada 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

Las autoridades competentes que tienen atribuidas las competencias del DNI y de los certificados de firma centralizada responderán 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, y 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 Autoridad Competente responderá por los daños y perjuicios que causen a cualquier ciudadano en el ejercicio de su actividad cuando incumpla las obligaciones que les 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 la Dirección General de la Policía (Ministerio del Interior), como prestador cualificado de servicios de confianza, informe debidamente a los ciudadanos 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 (Ministerio del Interior) 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 de la vigencia del certificado electrónico.
- La Dirección General de la Policía (Ministerio del Interior) como 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.

- La Dirección General de la Policía (Ministerio del Interior) no asumirá responsabilidad alguna por los daños derivados o relacionados con la no ejecución o la ejecución defectuosa de las obligaciones del ciudadano y/o del prestador de servicio.
- La Dirección General de la Policía (Ministerio del Interior) no será responsable de la utilización incorrecta de los Certificados ni las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información almacenada en el procesador de la tarjeta criptográfica del Documento Nacional de Identidad electrónico.
- La Dirección General de la Policía (Ministerio del Interior) 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 (Ministerio del Interior) 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 (Ministerio del Interior) no será responsable del contenido de aquellos documentos firmados electrónicamente por los ciudadanos con el Certificado del DNI y los certificados de firma centralizada.
- La Dirección General de la Policía (Ministerio del Interior) 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 ciudadanos 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 CIUDADANO

El ciudadano 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 ciudadano 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 ciudadano.

El Documento Nacional de Identidad electrónico es un documento personal e intransferible emitido por el Ministerio del Interior 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 Dirección General de la Policía (Ministerio del Interior), respecto de las Autoridades de Certificación del DNI y de los certificados de firma centralizada, no asumen 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.dnie.es/dpc
- WEB: http://pki.policia.es/dnie/publicaciones/dpc

Para los términos y condiciones del servicio de confianza

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

Para la Declaración de divulgación de la PKI (PDS)

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

6. POLÍTICA DE PRIVACIDAD

De acuerdo con la legislación española en materia de protección de datos, se recoge dentro del capítulo 11 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 DNI y de los certificados de firma centralizada. 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) del DNI Electrónico y de los certificados de firma centralizados.

Nombre	Grupo de trabajo del Certificado de Identidad Pública		
Dirección e-mail	certificados@dnielectrónico.es		
Dirección	C/Miguel Ángel 5 MADRID (España)		
Teléfono	+34913223400	**Fax**	+34913085774

Para la resolución de cualquier conflicto que pudiera surgir con relación a la DPC, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a la Jurisdicción Contencioso Administrativa.

8. NORMATIVA APLICABLE

Las operaciones y funcionamiento de DNI y de los certificados de firma centralizada estarán sujetas a la normativa que les sea aplicable y en especial a:

- 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.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).
- 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 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- Ley 84/78, 28 de Diciembre que regula la tasa por expedición y renovación del DNI.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- REAL DECRETO 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.
- Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma 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 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.
- Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.
- Real Decreto 414/2015, de 29 de mayo, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, Título I, Capítulo I, Artículos 3 y 4.
- Real Decreto 557/2011, de 20 de abril por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, Título XIII, Capítulo I, Artículos 205 y 206, Capítulo II, Artículos 207-210 y Capítulo IV, Artículos 213 y 214.
- Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España en ciudadanos de los Estados miembros de la Unión Europea y de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo.
- Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, concretamente ANEXO I Secretaria de Estado de Seguridad, Dirección General de Policía, Ámbito del Cuerpo Nacional de Policía, Punto 3: Adexttra.
- Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones, por las que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (entrada en vigor: 2 de Octubre de 2016).
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

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 del DNI y de certificados de firma centralizada de forma anual en conformidad con EN 319 411-2, de acuerdo con el Plan de Auditorías de la Autoridad Competente. Con ello se garantiza la adecuación de su funcionamiento y operativa con las estipulaciones incluidas en la Declaración de Prácticas y Políticas de Certificación.

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 Autoridad Competente 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.