tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

122

PROTECCIÓN DE DATOS PERSONALES, DNI-E Y PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN: ¿UN OBSTÁCULO PARA LA E-ADMINISTRACIÓN?

Julián Valero Torrijos
Departamento de Derecho Administrativo
Universidad de Murcia

Daniel Sánchez Martínez
Departamento de Ingeniería de la Información y las Comunicaciones
Universidad de Murcia

Julián Valero Torrijos
Daniel Sánchez Martínez

Palabras clave

Protección de datos personales, prestación de servicios de certificación, validación de certificados, DNI electrónico.

Resumen de su Comunicación

Esta comunicación analiza los riegos que plantea la implementación de los sistemas de identificación digitales y, en concreto, el DNI electrónico para la adecuada protección del derecho fundamental a la protección de los datos de carácter personalmente, especialmente por lo que se refiere a la gestión del sistema de validación del estado de los certificados. Los prestadores de servicios de certificación son terceras partes de confianza que manejan información personal acerca de la actividad realizada por los titulares de los certificados, encontrándose obligados a adoptar las medidas técnicas y organizativas necesarias que garanticen el adecuado tratamiento de la información obtenida en la prestación del servicio de validación de certificados. En esta comunicación se analizan las implicaciones que para la Dirección General de la Policía supone la puesta en marcha del DNI electrónico desde la perspectiva del estricto cumplimiento de las exigencias legales impuestas en materia de protección de datos personales por la Ley Orgánica 15/1999.

Julián Valero Torrijos
Daniel Sánchez Martínez

PROTECCIÓN DE DATOS PERSONALES, DNI-E Y PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN: ¿UN OBSTÁCULO PARA LA E-ADMINISTRACIÓN?

1. Modernización tecnológica de la Administración Pública e identificación de los ciudadanos. El papel del DNI-e

Aunque la problemática relativa a la protección de los datos personales en poder de las Administraciones Públicas ha planteado hasta ahora una singular relevancia en la medida que son precisamente este tipo de entidades quienes mayor información recopilan de los ciudadanos, lo cierto es que la proyección de la tecnología sobre su actividad nos obliga a tener que insistir de nuevo en ella, en especial para advertir que no todas las posibilidades que ofrece la tecnología son admisibles jurídicamente, sobre todo teniendo en cuenta las singulares finalidades a que ha de dirigirse la actividad administrativa. Una de las cuestiones que mayores debates ha suscitado en relación con la protección de los datos personales y los servicios administrativos en línea es la referente a las implicaciones que para aquel derecho pueda tener la utilización de sistemas de identificación digitales como el DNI electrónico, especialmente a partir de la configuración legal que este instrumento ha recibido en los artículos 15 y 16 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Si bien es cierto que se trata de un instrumento de gran utilidad para facilitar la gestión informativa referida a personas concretas, no lo es menos que la interconexión entre bases de datos diversas y heterogéneas en cuanto a su contenido y finalidad puede convertirse en un auténtico peligro para el derecho analizado por cuanto permite crear perfiles de aquéllas de forma sencilla, al menos para quien pueda tener acceso a esas múltiples fuentes informativas. Precisamente, en el caso del DNI electrónico ese acopio informativo se encuentra en manos de la Dirección General de la Policía o, en su caso, de las entidades privadas en quienes confíe la gestión de la lista de certificados revocados, tal y como dispone el artículo 12 del 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.

Precisamente, uno de los principales problemas que plantea el funcionamiento del DNI electrónico desde la perspectiva jurídica es el respeto a las exigencias normativas de la protección de los datos personales de los titulares de los certificados, especialmente por lo que se refiere a la consulta de la vigencia de aquéllos con ocasión de la ejecución de servicios de Administración electrónica: hasta tal punto que una deficiente articulación en la gestión de estos servicios puede convertirse en un obstáculo que dificulte gravemente [cuando no impida] la consolidación de este nuevo modelo de gestión administrativa basado en la tecnología. En la presente comunicación se analizan los flujos informativos que conlleva la utilización del DNI electrónico desde el punto de vista de la gestión relativa a la validación de los certificados de su titular, tanto por parte de la Administración Pública responsable del servicio telemático que requiere llevar a cabo tal comprobación como por parte del prestador de servicios de certificación que, en su momento, se encargue de realizar esta función respecto de los ciudadanos que deseen activar su identidad digital al solicitar la expedición o renovación del DNI.

2. El origen del problema: implicaciones técnicas de la validación de certificados

2.1. Diferentes tipos de validación de certificados: ventajas e inconvenientes

A.Validación off-line: distribución de listas de certificados revocados (CRL)

Se trata del método más tradicional en cuanto a mecanismos de validación de certificados se refiere. El prestador de servicios de certificación (PSC) genera, firma y publica de forma periódica estas listas, facilitando su descarga por parte de los clientes potenciales. Una CRL contiene una lista de todos los números de serie de certificados digitales revocados por ese PSC, junto a la causa de la revocación de cada uno de ellos, y la fecha y hora a la que se produjo. Además las CRLs están numeradas y tienen un periodo de validez que se especifica en las mismas. Transcurrido ese periodo el cliente debe descargar la nueva CRL.

Durante el ciclo de vida del PSC, la CRL crece en tamaño, existiendo dos posibilidades de diseño, o bien cada CRL sustituye a la anterior por completo, o bien complementa a la anterior almacenando únicamente los certificados revocados posteriores a la última publicación (delta-CRLs). Además las CRLs pueden fraccionarse en razón a distintos factores (uso, localización...).

El mecanismo de validación es muy sencillo. El cliente descarga la CRL en local, y posteriormente realiza todas las comprobaciones de estado de distintos certificados contra la lista descargada. Es por ello que a este tipo de validación se la denomina off-line. Se puede observar en la figura 1.

Figura 1. Validación de certificados mediante CRLs

La simplicidad del método ofrece una serie de inconvenientes evidentes. El primero es que la responsabilidad de descargar y actualizar las CRLs recae sobre el cliente. En caso de trabajar sobre una CRL no actualizada, no se podría la veracidad de las comprobaciones. El segundo es el aumento de la complejidad en la lógica de los clientes, que necesitan descargar, instalar e interpretar las listas, haciendo las comprobaciones de estado por ellos mismos. El tercero y más importante es el relativo a la periodicidad de las publicaciones. Es posible que en el intervalo de publicación entre una lista y otra, un certificado pase a un estado revocado, y en cambio la validación del mismo siga siendo correcta. Se trata, por tanto, de un mecanismo poco fiable para entornos de aplicación donde la validación sea un factor crítico.

B. Validación on-line: Online Certificate Status Protocol (OCSP)

A día de hoy, este protocolo constituye el mecanismo de validación on-line más extendido, y alternativo al uso de distribución de listas CRL. Su diferencia fundamental es que la responsabilidad de la comprobación del estado del certificado se traslada a un servicio OCSP Responder.

El cliente construye solicitudes de comprobación de estado de acuerdo al protocolo, en las que se envía el identificador del certificado a comprobar. El servicio OCSP Responder trata cada petición y devuelve respuestas firmadas con el estado del certificado, en las que se incluye el instante preciso de las comprobaciones (figura 2). La naturaleza on-line de este mecanismo de validación permite asegurar que cada respuesta [illegible] de fiabilidad de las CRLs.

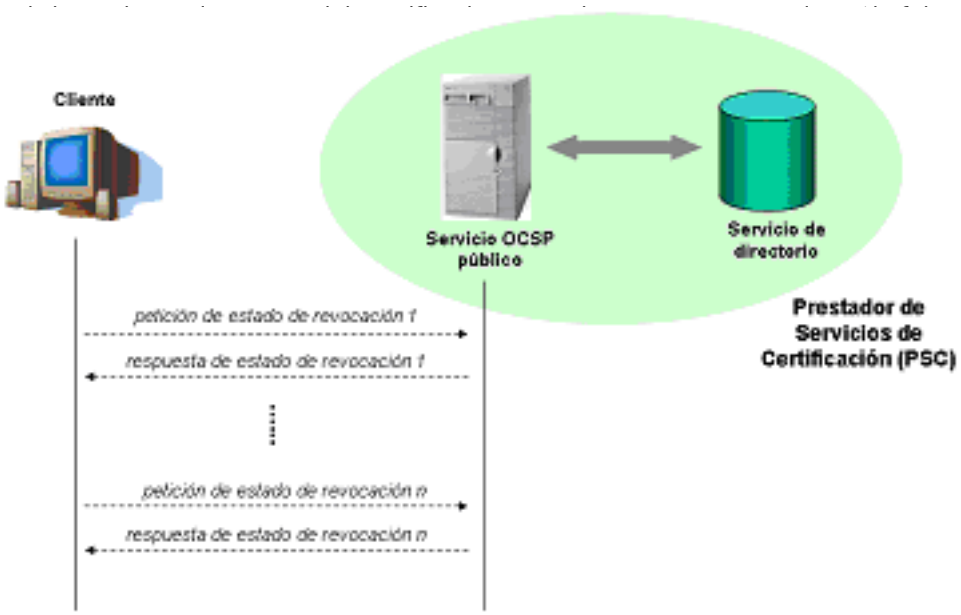

Figura 2. Validación de certificados mediante OCSP

2.2. Servicios de Administración electrónica y validación de certificados: un riesgo potencial para la protección de los datos de carácter personal

En los siguientes apartados se analizará en detalle el proceso de validación de un certificado digital en servicios de Administración electrónica, y en función del mecanismo de validación utilizado, prestando especial atención a las implicaciones en cuanto a privacidad que de este proceso se derivan. En los procesos de Administración electrónica siempre aparecen tres actores clave; el usuario en posesión de una credencial electrónica, el propio servicio telemático ofrecido por una Administración, y un tercero de confianza (TTP) que ofrece información de validación de la credencial del usuario a la Administración.

En España el escenario típico que se encuentra es el de un usuario, sin conocimientos tecnológicos, y en posesión de un DNI electrónico emitido por el Ministerio del Interior. El DNI electrónico contiene dos certificados reconocidos; un certificado de autenticación, que permite la identificación del usuario frente a un servicio, y un certificado de no repudio, que permite realizar procesos de firma electrónica sobre documentos electrónicos.

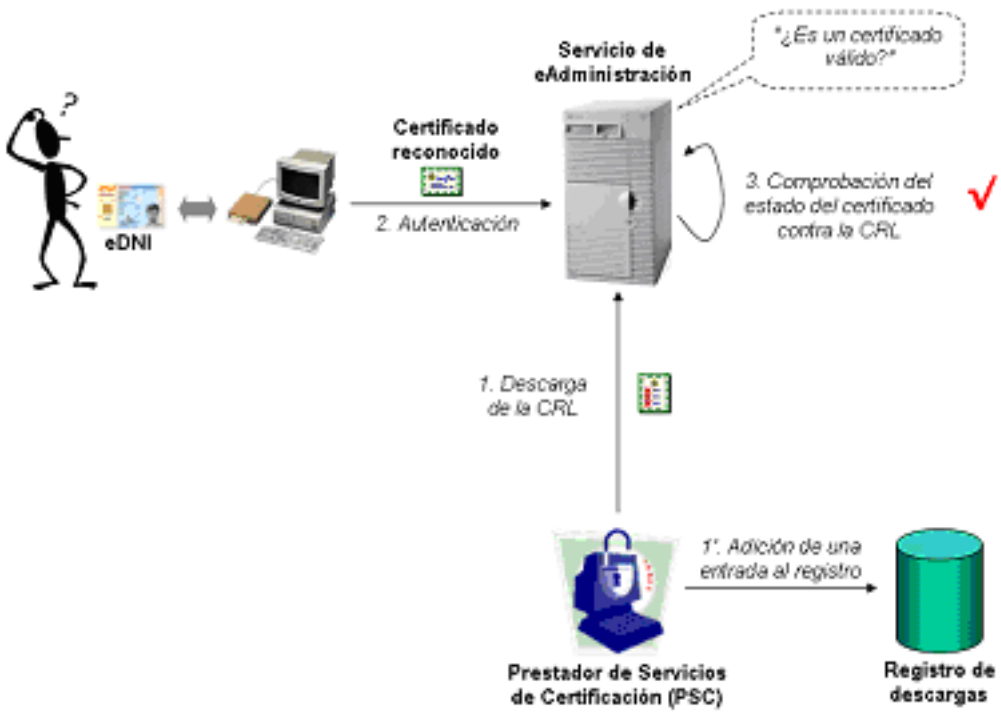

Figura 3. Escenario de e-Administración I. CRLs.

En una gran parte de las ocasiones el usuario desconoce tanto la información exacta contenida en los certificados de su DNI electrónico, como los flujos de información que se generan cuando inserta su DNI en un lector de tarjetas de un ordenador para acceder a un determinado portal de la Administración. El usuario tampoco es consciente de la existencia de un TTP, ni de la interacción que la Administración tiene con el mismo con el objetivo de conocer la validez de la credencial que ha presentado. Por último, tampoco conoce que el TTP suele almacenar información sobre el uso de sus servicios, tanto por motivos estadísticos, como por seguridad y control de posibles ataques al sistema.

A. Servicios de Administración electrónica y CRLs

En la figura 3 se puede observar el flujo fundamental de información entre los distintos actores descritos, en un escenario habitual en el que la validación de certificados se realiza mediante el uso de CRLs. En primer lugar, y previo a cualquier uso del servicio por parte de un usuario, el administrador del servicio deberá descargar e instalar la CRL que le proporciona el PSC, procedimiento éste que puede ser automatizado para que se realice de forma periódica, y en función de la frecuencia de publicación de nuevas CRLs por parte del PSC. Cada vez que el servicio descarga una nueva CRL, el PSC puede añadir una entrada al respecto en un registro relativo a la descarga de CRLs, teniendo constancia en todo momento de qué servicios de Administración electrónica hacen uso de su mecanismo de validación off-line (tabla 1).

Fecha - Hora	Descarga de CRLs
12/02/2006 09:11	Servicio eAdministración 1
12/02/2006 10:07	Servicio eAdministración 5
...	...
13/02/2006 09:12	Servicio eAdministración 1

Tabla 1. Registro de descargas de CRLs

Una vez configurada la CRL de forma local, el servicio se encontrará operativo para todos los usuarios del sistema. El usuario introducirá su tarjeta de identificación electrónica (DNI) en el lector de tarjetas inteligentes de un ordenador personal e intentará acceder al servicio de Administración electrónica. Para ello el certificado de identificación del usuario es extraído de su DNI y enviado al servicio durante el proceso de autenticación. El servicio, una vez recibe la credencial, procede a comprobar la validez de la mismo, para lo cual chequea, de forma local, si el certificado del usuario se encuentra dentro de la lista de certificados revocados (CRL) que guarda localmente. Si el certificado no se encuentra en la misma, podrá concluir que es una credencial válida, y permitirá el acceso del usuario, ya plenamente identificado, a la funcionalidad del servicio.

Las sucesivas peticiones de servicio por parte de los usuarios se resolverán de la misma forma, volviendo a comprobar el estado del certificado del usuario contra la CRL local. La política de funcionamiento que tenga establecida el servicio permite definir la periodicidad de descargas de nuevas CRLs, críticas para asegurar la vigencia de las validaciones.

B. Servicios de Administración electrónica y OCSP

En este segundo escenario, representado en la figura 4, se observa un flujo de información parcialmente diferente al anterior, debido a la naturaleza on-line de la operación de comprobación del estado del certificado. Inicialmente el proceso se desarrolla de una forma equivalente al escenario anterior, recibiendo el servicio el certificado de identificación contenido en el DNI. A continuación el servicio realiza una operación de obtención del número de serie del certificado de usuario a partir del mismo, y envía esta información al PSC a través de una petición OCSP de comprobación del estado del certificado. El PSC devuelve una respuesta OCSP al servicio de Administración electrónica, verificando o no la validez del certificado asociado al número de serie consultado.

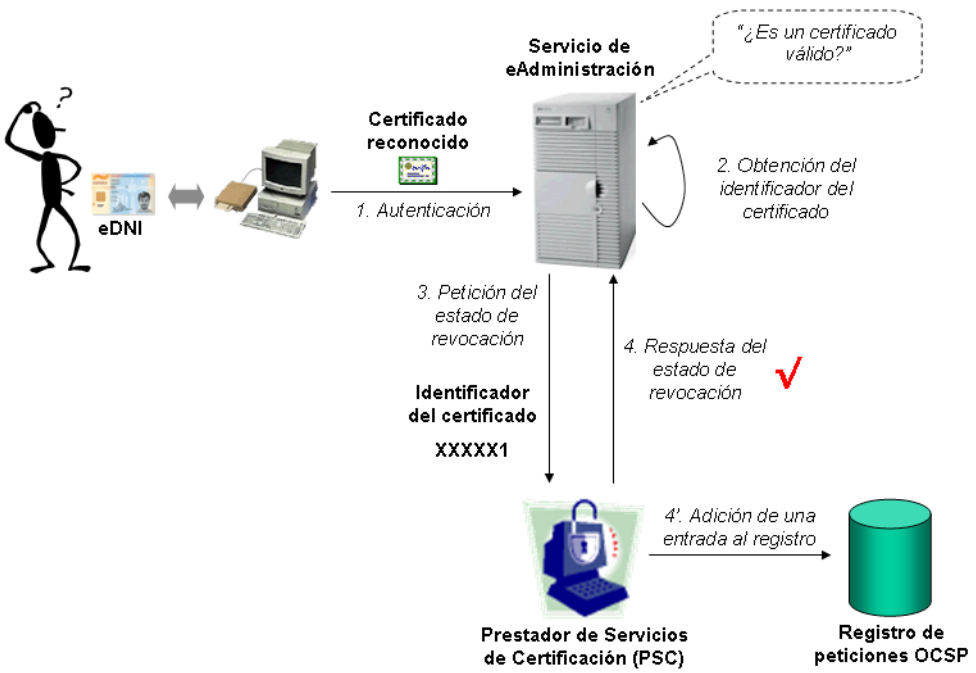

Figura 4. Escenario de e-Administración II. OCSP

Al mismo tiempo, el PSC, puede almacenar la información relativa a la petición recibida, consistente en el identificador del servicio solicitante, el número de serie del certificado comprobado, y el instante exacto de la consulta. Las sucesivas solicitudes de validación pueden generar las correspondientes anotaciones en el registro de solicitudes OCSP, tal y como se puede observar en la tabla 2. Por tanto, este mecanismo de validación posibilita que el PSC mantenga un registro exacto del número de serie de los certificados que un servicio de Administración electrónica ha comprobado en su ciclo de vida, pudiendo además conocer el número de comprobaciones totales sobre cada uno de esos certificados y la fecha y hora a la que se produjeron.

Fecha - Hora	Servicio	Certificado
12/02/2006 09:11	Servicio eAdministración 1	00001
12/02/2006 10:07	Servicio eAdministración 5	03670
...	...	
13/02/2006 09:12	Servicio eAdministración 1	00434

Tabla 2. Registro de peticiones OCSP

Habitualmente un PSC está compuesto por varias entidades y servicios, que cubren el ciclo de vida de un certificado digital (autoridad de registro, directorio de publicación de certificados, servicio de solicitud, autoridad de validación, servicio de validación, servicio de revocación...). Es por ello que el PSC dispone, por un lado, de la información relativa a cada uno de sus certificados (contenida en el servicio de directorio), y, por otro lado, puede disponer de los registros de solicitudes de comprobación del estado de los certificados generados por su servicio de validación de certificados. La relación de ambas fuentes de información sustenta la posibilidad técnica de generar informes relativos a los usuarios y su uso de los servicios de

Administración electrónica. Por ejemplo, se podrían obtener informes indexados por usuario, con las fechas y horas de utilización de cada servicio (figura 5), o informes indexados por servicio, con las fechas y horas en que cada usuario ha accedido al mismo.

Figura 5. Ejemplo de informe de actividad de un usuario

3. El enfoque legal: protección de los datos personales en el ámbito de la prestación de servicios de certificación

Desde una perspectiva jurídica, el principal problema que plantean los sistemas de identificación basados el uso de certificados digitales está relacionado con el respeto de las exigencias sobre protección de datos personales. En concreto, tal y como sucede con el DNI-e, dichos certificados presentan una doble función ya que, por una parte, de conformidad con lo dispuesto en el artículo 15 LFE, sirven como herramientas para la identificación del titular en las relaciones telemáticas; y, por otra parte, permiten asimismo garantizar la autenticidad e integridad de los documentos rubricados. En ambos casos, el adecuado funcionamiento del sistema precisa la intervención de una tercera parte de confianza, el prestador de servicios de certificación, y que se encarga de la expedición de los certificados a los usuarios, respondiendo, en su caso, de que los mismos hayan sido generados de forma segura y de que se encuentren en vigor, para lo cual ha de proporcionar la información relativa a la eventual revocación del certificado tal y como requiere el artículo 10 LFE. Así pues, el acceso a la lista de certificados revocados constituye uno de los elementos clave en torno al cual gira la prestación de servicios de certificación.

En el caso de los servicios administrativos en línea, cuando la Administración Pública con la que se pretende entablar el contacto necesita conocer si el certificado electrónico empleado está todavía en vigor, a los efectos de determinar si todavía puede confiar en la identidad del usuario, deberá realizar la oportuna consulta al PSC pues, de lo contrario, asumirá las consecuencias que puedan derivarse de su previa revocación. Los peligros potenciales desde la óptica del derecho de los ciudadanos a la protección de los datos personales son, por tanto, más que evidentes en la medida que una incorrecta implementación del sistema de consulta de los certificados revocados puede determinar un tratamiento inadecuado y excesivo contrario al artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal.

En efecto, si el PSC optara por integrar en un sistema de información tanto los datos relativos al certificado en sí mismo considerado y a su titular como la información relativa a la gestión de los certificados revocados, nos encontraríamos con que estaría en disposición de conocer cuáles son las actividades llevadas a cabo por el usuario en sus relaciones con las Administraciones Públicas y, en su caso, con las entidades privadas con las que entable comunicaciones electrónicas a través del DNI-e. Así pues, en la medida en que el conocimiento de esta información resulta manifiestamente innecesaria para la prestación del servicio de certificación, no estaría justificado que el prestador pudiera tomar conocimiento de la misma y, en consecuencia, está obligado a configurar el acceso a la lista de certificados revocados de forma disociada incluso para él mismo, sin que en modo alguno pueda almacenar la información temporal que recibe con ocasión de las consultas acerca de la vigencia de los certificados.

En otras palabras, la autoridad de certificación debería desvincular la información relativa a los certificados cuya vigencia ha finalizado de la identidad de sus titulares respectivos, tanto en la gestión interna del servicio que presta como por lo que se refiere a la publicidad de la lista de certificados revocados ya que, en este último caso, el tratamiento consistente en asociar la identidad del usuario a su correspondiente certificado únicamente podría realizarlo la Administración Pública titular del servicio administrativo en línea, siempre con el escrupuloso respeto de los principios generales fijados en la LOPDP y demás normas vigentes en la materia. Pues bien, teniendo en cuenta que el DNI-e presupone que todos los ciudadanos que soliciten su activación pasen a ser usuarios de un servicio que, en última instancia, depende del Ministerio del Interior, a través de la Dirección General de la Policía, a tenor de lo dispuesto en los artículos 3.2 y 12.2 del Real Decreto 1553/2005.

Así pues, a menos que se estructuren de forma separada la base de datos propia de los certificados y la relativa a los que se encuentran revocados y se garantice adicionalmente que no se archiven las consultas realizadas en esta última, un eventual problema de seguridad permitiría confeccionar un completísimo perfil de los ciudadanos por lo que se refiere a sus actividades telemáticas en las que utilice el DNI-e. Teniendo en cuenta el carácter gratuito de este servicio y el apoyo institucional del que goza al estar respaldado por el Estado, no es difícil aventurar que un gran número de ciudadanos soliciten la activación de sus certificados digitales con ocasión de la expedición o renovación de su DNI.

4. Conclusiones

Nos encontramos, por tanto, ante un peligro cierto que puede afectar seriamente a la confianza de los ciudadanos en la seguridad jurídica de la Administración electrónica y comprometer seriamente no sólo su consolidación sino, sobre todo, la futura implementación de nuevos servicios administrativos telemáticos. Aunque con carácter general el artículo 6 LOPDP habilita el tratamiento de los datos personales por parte de los responsables de los ficheros cuando cuenten con el consentimiento de los titulares, el carácter voluntario de los servicios de certificación electrónica asociados al DNI-e consagrado en los artículos 9.2 y 17 del Real Decreto 1553/2005, no puede considerarse suficiente a estos efectos en la medida que se vincularía el consentimiento prestado con una defectuosa prestación del servicio de validación de los certificados manifiestamente contrario al contenido esencial del derecho a la protección de los datos personales ya que nos encontraríamos ante un tratamiento ilícito.

En consecuencia, el tratamiento de datos personales vinculado a la prestación de servicios de certificación y, en concreto, a la comprobación de la vigencia de los certificados alojados en el DNI-e ha de implementarse con pleno respeto a la normativa sobre protección de datos y, por lo que se refiere a la perspectiva técnica, de las medidas de seguridad que se acaban de referir en aplicación de lo dispuesto en el artículo 9 LOPDP y su normativa de desarrollo.