



Introducción

La Administración Pública Española tiene un objetivo prioritario con su incorporación a la Sociedad de la Información de acuerdo a lo establecido en la Ley 11/2007, que no es otro que producir una modernización del modelo de organización y prestación de servicios, orientándolo a desarrollar nuevas y más modernas iniciativas a través de nuevos canales de comunicación y cuya finalidad sea mejorar la calidad de las actuaciones que se realizan, y agilizar la relación Ciudadano-Empresa-Administración en el marco de la Administración Electrónica.

En este sentido, el Servicio Público de Empleo Estatal (SPEE), consciente de esta nueva situación, ha puesto en marcha la Web REDTRABAJ@ que introduce una manera más dinámica de gestionar la búsqueda de empleo, actuando como verdadero punto de encuentro entre las empresas que ofrecen trabajo y los demandantes que buscan empleo y, asimismo, contempla la posibilidad de llevar a cabo diversos trámites electrónicos como por ejemplo que la persona desempleada pueda realizar el auto-reconocimiento de la prestación por desempleo a través de Internet.

REDTRABAJ@ permite al SPEE entrar de lleno en la Administración electrónica, cumpliendo con la Ley 11/2007, de modo que se acercan los servicios ofrecidos a los ciudadanos, evitando desplazamientos y tiempos muertos de espera, mejorando la calidad del servicio recibido por la ciudadanía.

No obstante, para que dicha calidad del servicio sea realmente percibida como tal, es imprescindible garantizar el cumplimiento de las distintas disposiciones inherentes a la e-Administración y en especial la Ley 11/2007, evitando la brecha digital en cuanto a las formas de identificación y autenticación, y contemplando no solamente el uso del certificado digital sino también otros mecanismos, tales como claves concertadas en un registro previo (usuario/contraseña), al tiempo que se garantiza la integridad y el no repudio de las transacciones realizadas y se minimiza la posibilidad de fraude electrónico por suplantación de personalidad digital que el mecanismo usuario/contraseña conlleva. La solución incorporada para esta finalidad se basa en tecnología de PKI de ENTRUST.

Asimismo, para desplegar esta nueva Plataforma de Seguridad para usuarios externos se instalaron Servidores con tecnología de Proxy Inverso que permiten identificar y autenticar, y posibilitan el acceso a los diferentes servicios y aplicaciones, quedando éstos ya no para la función del perfilado sino para el negocio propiamente dicho, confiando esta funcionalidad en NOVELL Access Manager.



Finalmente, se debe contemplar la correcta conservación y custodia de la documentación electrónica asociada a los procedimientos administrativos realizados de manera que se asegure tanto la integridad física de los mismos, como la vigencia de la firma electrónica utilizada, y se garantice la plena validez legal a lo largo del tiempo. A tal fin se incorporó el Sistema de Custodia del Grupo SIA.

Justificación de la necesidad

La Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa en condiciones de seguridad jurídica.

El marco normativo español ha incluido en los últimos años legislación muy orientada al fomento del uso de las nuevas tecnologías entre las que destacan la Ley 59/2003: Ley de Firma Electrónica y la ya mencionada Ley 11/2007. Al amparo de las Leyes de impulso de la sociedad de la información, las Administraciones y organizaciones están impulsando Portales para la prestación de servicios a través de Internet que tradicionalmente se ofrecen de manera presencial.

Para todos estos nuevos servicios se exige al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos. Estas garantías de seguridad deberán ser proporcionales a la naturaleza y circunstancias de los trámites o actuaciones a realizar. Así, los ciudadanos o empleados públicos deberán poder utilizar alguno de los siguientes mecanismos de identificación o firma electrónica:

- DNIe. Firma Electrónica incorporada con el nuevo Documento Nacional de Identidad Electrónico.
- Firma Electrónica Avanzada, incluyendo la posibilidad de basarla en certificados reconocidos.
- Otros sistemas de Firma Electrónica, como la utilización de un identificador y contraseña obtenidos en un proceso de registro previo del usuario.

La Ley 11/2007 recoge las siguientes definiciones de Firma Electrónica:

- Firma Electrónica Básica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados a ellos, que pueden ser utilizados como medio de identificación del firmante.



- Firma Electrónica Avanzada. Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Firma Electrónica Reconocida. Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Aunque los tres tipos de firma mencionados son firmas electrónicas es conveniente establecer que:

- Firma Electrónica Básica. Este tipo de firma electrónica se basa, por ejemplo, en un secreto compartido como una pareja de claves tipo usuario/contraseña. Permite identificar al firmante pero no establece una vinculación objetiva entre el documento firmado y el contenido del mismo.
- Firma Electrónica Avanzada. Este tipo de firma es la basada en un certificado digital X.509v3 que permite identificar al firmante y establece una vinculación objetiva entre el documento firmado y el contenido del mismo que garantiza su integridad y el no repudio de la transacción.
- Firma Electrónica Reconocida. Este tipo de firma se basada en un certificado digital X.509v3 emitido por una Autoridad de Certificación Reconocida. Permite identificar al firmante, garantizar la integridad del documento y es equiparable a la firma manuscrita.

Por lo tanto, la Ley 11/2007 cuando relaciona el mecanismo de identificación del ciudadano y la autenticación de su actuación, establece que en los supuestos de utilización del DNIe o de un sistema de firma electrónica avanzada, la autenticación de la actuación se garantiza por el uso del propio certificado digital X509v3 en el que están basados ambos sistemas, al vincular de manera objetiva el documento firmado y el contenido del mismo garantizando la integridad y el no repudio de la transacción.

Sin embargo, la Ley 11/2007 establece que en aquellos supuestos de utilización de otros sistemas de Firma Electrónica, caso del usuario/contraseña de un registro previo, al no poderse establecer vinculación objetiva entre el documento firmado y el contenido del mismo, será la propia Administración Pública la que garantice la integridad y el no repudio por ambas partes de los documentos electrónicos concernidos.



De este modo, la Ley 11/2007, de manera explícita en unos casos (DNIe o sistema de firma electrónica avanzada) o de manera implícita en otros (usuario/contraseña en registro presencial), requiere la utilización de un sistema de Firma Electrónica Avanzada, que permita identificar al firmante y establecer una vinculación objetiva entre el documento firmado y el contenido del mismo que garantiza su integridad y el no repudio de la transacción.

Asimismo, este sistema de Firma Electrónica Avanzada debe poder ser compatible con que el usuario utilice como identificación una pareja de claves usuario/contraseña concertada en un registro previo.

Objetivos

A la vista de las necesidades expuestas anteriormente y en aras de proporcionar un servicio lo más universal posible, se hace necesario contemplar las medidas de seguridad adecuadas para que la Web REDTRABAJ@ permita todos los supuestos de identidad digital de la Ley 11/2007, de modo que el ciudadano pueda utilizar en sus relaciones administrativas por vía electrónica con el SPEE, aquél en el que se sienta más cómodo, sin que existan barreras para su utilización por medios o conocimiento, al tiempo que se garantiza plena validez legal.

En este sentido, se han establecido tres líneas de actuación complementarias entre sí para conseguir el objetivo global planteado:

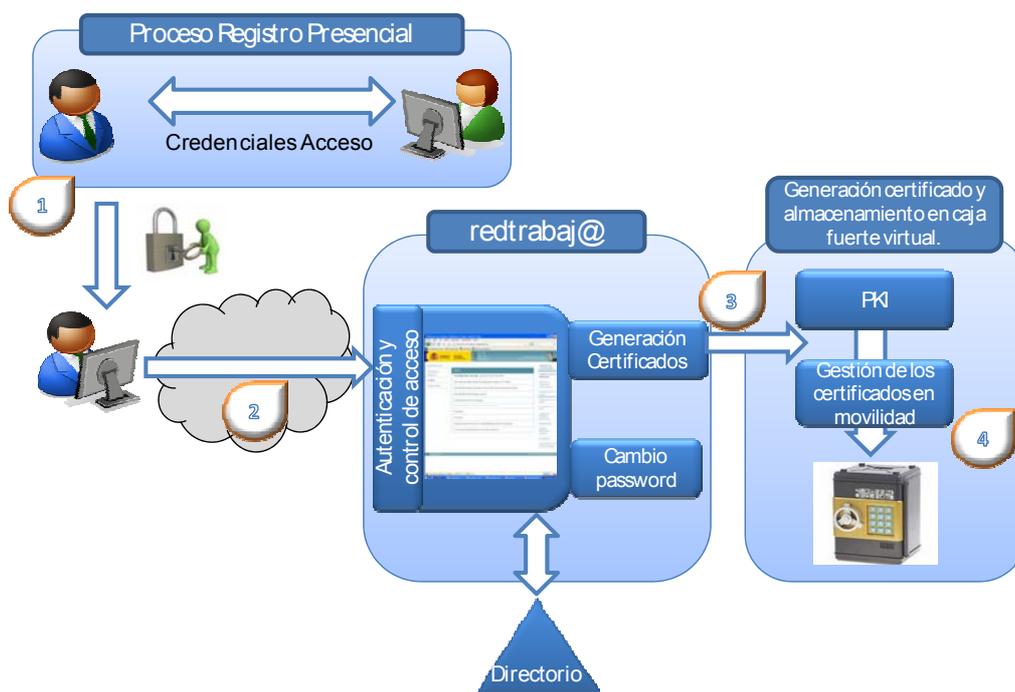
- Sistema de identificación y control de acceso al Portal REDTRABAJ@ que permite llevar a cabo la autenticación del usuario contemplando los distintos tipos de credenciales soportados: DNIe, certificados digitales emitidos por una autoridad de certificación reconocida, usuario y contraseña entregados en el registro realizado en las oficinas del SPEE.
- Sistema de certificado digital, exclusivo para firma de documentos, con almacenamiento blindado y código de confirmación de uso: Para aquellos usuarios que se identifican con usuario/contraseña en la Web REDTRABAJ@, situación contemplada en la disposición primera del artículo 16 de la Ley 11/2007, es necesario garantizar, de acuerdo a lo establecido en la disposición segunda de dicho artículo, la integridad y no repudio por ambas partes de los documentos electrónicos.

- Para ello, se propone la utilización de un sistema de emisión de certificados digitales exclusivos para firma digital de documentos electrónicos con almacenamiento en caja fuerte virtual que permite el acceso del usuario al mismo en movilidad sin estar sujeto a su instalación en un equipo concreto.
- Como complemento a dicho sistema se utiliza un sistema de segundo factor de autenticación consistente en el envío de un código de confirmación de la operación de firma del documento a través de SMS al teléfono móvil del ciudadano.
- Sistema de custodia de documentos electrónicos: los documentos electrónicos requieren, del mismo modo que los generados en papel, de una protección y garantía de validez futura. La posibilidad de permitir a los ciudadanos la realización de trámites administrativos a través de redtrabaj@ utilizando firma electrónica, conlleva implantar una solución de custodia de documentos electrónicos que permita fundamentalmente garantizar la no modificación del documento electrónico con carácter posterior a su firma y que la firma digital realizada mantenga su inviolabilidad, aun cuando el paso del tiempo y los sucesivos avances tecnológicos en capacidad de procesamiento permitan romper las claves utilizadas a día de hoy en la firma de dicho documento electrónico.

Descripción funcional

A continuación se explica el funcionamiento del sistema tanto en la inicialización del mismo en el momento del registro como en su funcionamiento habitual cuando el ciudadano accede al Portal REDTRABAJ@ para realizar sus gestiones.

En lo referente al proceso de inicialización, la secuencia de acontecimientos es:



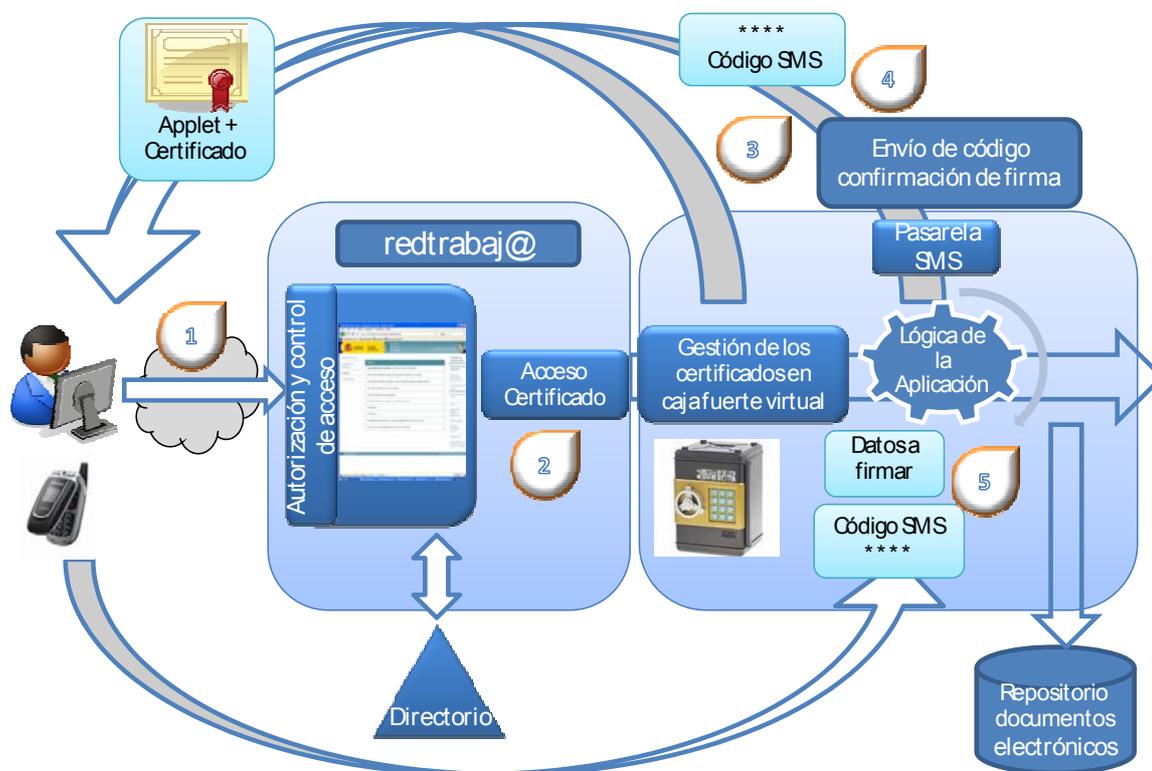
- 1) El ciudadano acude a la oficina del SPEE para registrarse como demandante de empleo y se le entrega un usuario/contraseña para que pueda acceder a la Web REDTRABAJ@ y, entre otras, pueda realizar el auto-reconocimiento electrónico de la prestación por desempleo.
- 2) El ciudadano accede a REDTRABAJ@ desde cualquier ordenador con conexión a Internet que cumpla con los requisitos técnicos mínimos que el Portal establece en cuanto tipo de navegador utilizado, versión empleada, etc.

Una vez enlazado al Sistema de Identificación, el ciudadano debe acceder para activar el usuario y contraseña que le han entregado siendo recomendable que se le obligue a cambiar la contraseña por motivos de seguridad.

Obviamente, el paso anterior no es necesario cuando el ciudadano va a acceder al Portal REDTRABAJ@ utilizando su DNIe o cualquier otro tipo de certificado digital reconocido, mecanismos de identificación que también están contemplados.

- 3) Si el ciudadano va a utilizar su usuario/contraseña y desea realizar trámites administrativos, este primer acceso, tras ser informado convenientemente y recabar su aprobación, el sistema de seguridad implantado realiza la emisión de un certificado digital X509v3 utilizando los datos del ciudadano.
- 4) Dicho certificado digital se almacena de manera blindada en una caja fuerte virtual, lo que permite el acceso a la misma con total movilidad por parte del ciudadano permitiéndole disponer de un sistema de firma electrónica avanzada al que accede con su usuario/contraseña obtenido en el registro del SPEE.

Una vez que el usuario se ha inicializado en el sistema este ya puede comenzar a realizar las operaciones específicas de REDTRABAJ@ entre ellas la realización de trámites administrativos como el auto-reconocimiento electrónico de la prestación por desempleo:



- 1) El ciudadano accede al Portal REDTRABAJ@, desde cualquier ordenador con conexión a Internet únicamente con las limitaciones impuestas por el propio Portal, e introduce su usuario/contraseña.

El ciudadano también puede acceder al Portal REDTRABAJ@ utilizando su DNIe o cualquier otro tipo de certificado digital reconocido mecanismos de identificación que también están contemplados

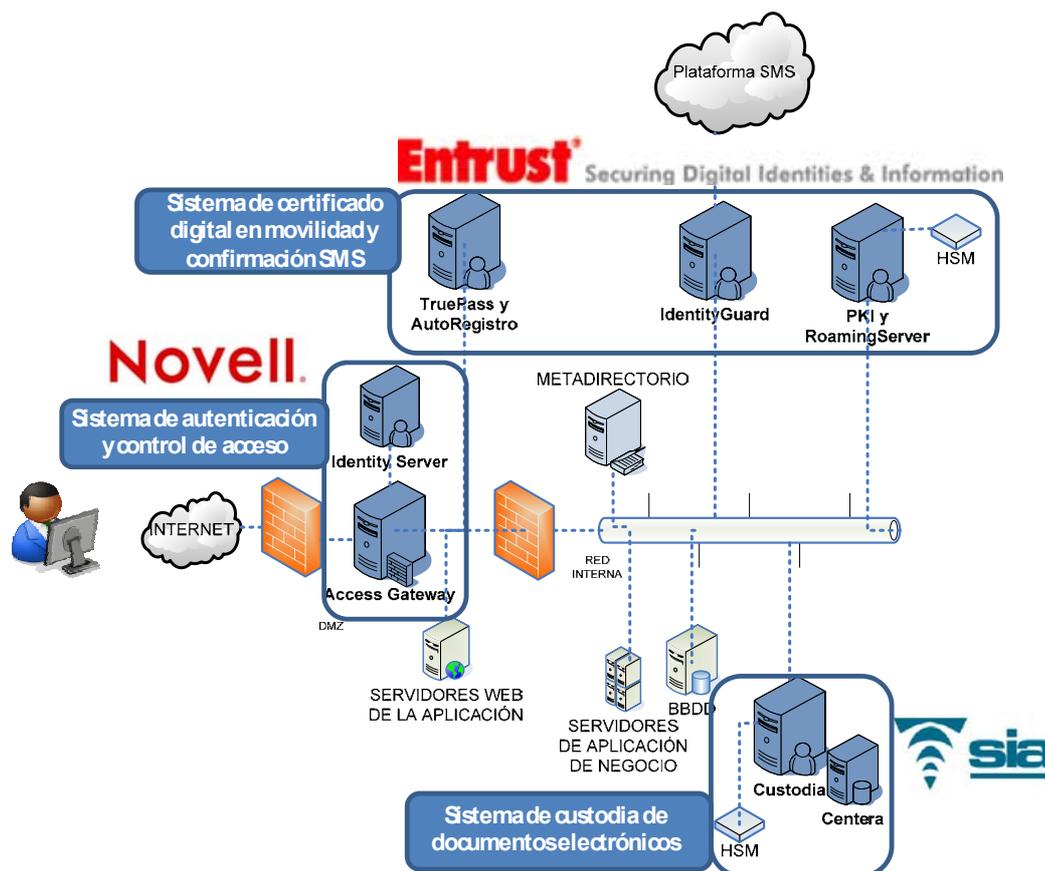
- 2) Esta acción conlleva el establecimiento de una sesión de navegación segura en la que se accede a la caja fuerte virtual donde el ciudadano tiene depositado el certificado electrónico X509v3 de firma electrónica avanzada que va a utilizar.
- 3) Dicho certificado se descarga en tiempo de navegación mediante un applet al ordenador donde está conectado el usuario y se ubica en una zona de memoria segura del navegador utilizado, únicamente existente durante la sesión de navegación establecida. De este modo, se garantiza una completa seguridad del sistema ya que ningún elemento externo a la sesión de navegación puede acceder al certificado y este se elimina completamente del ordenador sin dejar ningún rastro en el mismo una vez finalizada la misma.
- 4) El ciudadano pasa a realizar sus operaciones en el Portal REDTRABAJ@, hasta el momento en que desea realizar un trámite que requiere firma digital. En ese momento, se le presentan los datos a firmar junto con un campo donde debe introducir el código de confirmación de firma. Dicho código de confirmación se genera en tiempo real y se envía al teléfono móvil del ciudadano (obtenido durante el registro en la oficina del SPEE) mediante un SMS, a través de una pasarela existente en el SPEE.

De este modo, se evita el uso fraudulento del usuario/contraseña del ciudadano por terceras partes que se hayan podido hacer con el mismo utilizando mecanismos de ingeniería social, troyanos instalados en el ordenador, etc.

- 5) Una vez confirmada la operación de firma con el código recibido en el móvil, se procede a la firma del documento con el certificado del ciudadano y a su posterior post-proceso antes de ser enviado al sistema de custodia de documentos electrónicos. Finalizada la sesión, el certificado del ciudadano desaparece del ordenador utilizado, quedando únicamente disponible en su caja fuerte virtual para próximas conexiones.

Tecnología utilizada

Los componentes tecnológicos para la puesta en marcha del sistema anteriormente descrito son los que se muestran a continuación:



El Sistema de identificación y control de acceso al Portal REDTRABAJ@ está basado en la tecnología Novell utilizando los siguientes productos:

- Novell Access Manager: valida la identidad de los usuarios por medio de alguno de los sistemas de autenticación soportados: DNIe, certificado electrónico, usuario/contraseña; y controla el acceso en base a la identidad de los usuarios.
- Novell e-Directory: conforma el metadirectorio de identidades donde se almacenan las claves usuario/contraseña en el momento del registro del ciudadano y donde se valida su acceso cuando accede al Portal.



El Sistema de certificado digital, exclusivo para firma de documentos, con almacenamiento blindado y código de confirmación de uso está basado en la tecnología Entrust:

- Entrust Authority Security Manager: Implementa la autoridad de certificación que emite los certificados digitales basado en el estándar X.509, realiza el registro de los usuarios, mantiene la lista de certificados revocados y lleva a cabo la gestión de los certificados en movilidad (roaming). Está Certificado Common Criteria EAL 4+.
- Entrust Truepass: Permite la utilización de los certificados desde cualquier ubicación sin necesidad de tener ningún componente en el puesto de trabajo mediante un Applet (JAVA) que se descarga en tiempo de ejecución. Certificado FIPS 140-2 Level 1.
- Entrust IdentityGuard: Implementa un segundo factor de autenticación que permite evitar la suplantación de la identidad del usuario con un fin fraudulento mediante algo que el usuario conoce (usuario/contraseña) y algo que tiene que poseer (teléfono móvil)

El Sistema de custodia de documentos electrónicos está basado en la solución tecnológica del Grupo SIA:

- SIAVAL Custodia: Permite la custodia de los documentos electrónicos y las políticas de acceso asociadas llevando a cabo el resellado automático de los documentos firmados para garantizar su validez a lo largo del tiempo.
- Sistema de almacenamiento Centera: Repositorio físico con tecnología CAS (Content Address Storage) que garantiza la correcta conversación e integridad física del documento electrónico.

Los requisitos del ordenador del usuario que accede al Portal REDTRABAJ@ para poder utilizar la solución son los siguientes:

- Máquina virtual Java que se descarga e instala una sola vez de manera transparente.
- El cliente de firma utilizado por la solución propuesta (Entrust Truepass) es un Applet de Java ligero (180Kb) y se descarga de manera transparente.

Beneficios

La Plataforma de Seguridad de la Web REDTRABAJ@ del SPEE descrita con anterioridad presenta los siguientes beneficios:

- **Aumento de la Seguridad** al definirla y controlarla de forma centralizada, permitiendo un **ahorro de costes** en la administración y mantenimiento de la seguridad, y en el desarrollo y evolución de las aplicaciones de negocio.
- **Acceso seguro** a los recursos disponibles en la Web Redtrabaja, proporcionando autenticación, autorización y single-sign-on.
- Garantía de la **integridad de los documentos** tanto desde el ciudadano como desde el SPEE y por tanto el **no repudio de la transacción** realizada.
- **Evita la brecha digital** a los ciudadanos no habituados al uso de certificados electrónicos.
- **Minimiza el fraude** y permite demostrar en el tiempo la realización de la transacción al existir un documento firmado no ligado a la aplicación y sus futuras versiones.
- **Movilidad del ciudadano** al no estar ligada la conexión a un ordenador concreto: hogar, cibercafé, cajeros e-administración, etc.
- **Neutralidad tecnológica** al no estar ligada la ejecución en cliente a una tecnología de navegador concreta (Applet Java vs. ActiveX) ni a sistemas operativos (Windows, Linux o MAC).
- **Segundo factor de autenticación multifactorial**: móvil, correo electrónico, tarjeta coordenadas, etc.
- **Validez de los documentos electrónicos** en el tiempo, y prueba frente a terceros.

Conclusiones

- La Ley 11/2007 contempla diferentes mecanismos de identificación de los ciudadanos en los Portales de Servicios Electrónicos: DNIe, firma electrónica avanzada incluyendo certificado reconocido (FNMT etc.), claves compartidas en un registro como usuario/contraseña.
- La Ley 11/2007 establece que la Administración Pública debe garantizar la integridad de los datos aportados y el no repudio de la transacción por lo que se requiere utilizar firma electrónica avanzada aun cuando la identificación del ciudadano se realice mediante usuario y contraseña
- El sistema propuesto emite certificados digitales de uso exclusivo para firma electrónica avanzada con el SPEE que son almacenados en una caja fuerte virtual a la que solo puede acceder el usuario con su usuario/contraseña, y que solo se puede utilizar con un código de confirmación mediante SMS enviado al teléfono móvil del usuario.
- El sistema propuesto no introduce complejidad adicional ni en el Portal de Servicios ni en las aplicaciones existentes ni tampoco degradación de los tiempos de respuesta. El sistema de registro es flexible y adaptable a la Organización (registro presencial, registro en base a información previa aportada por el ciudadano que es confiable, registro en base a DNIe, ...)
- El sistema es independiente de la tecnología utilizada por el usuario, le permite total movilidad al no requerir ningún componente en el puesto de trabajo, y no requiere su involucración en la renovación del certificado una vez expirado ya que se renueva de manera automática.