

los certificados digitales de la FNMT-RCM

Aplicaciones y nuevos servicios



Por Felipe Amores Molero
Director de Sistemas de Información
Fábrica Nacional de Moneda y Timbre



En España, tanto las distintas Administraciones como las Empresas han apostado decididamente por Internet, creando numerosas Webs con información de interés público y poniendo a disposición de la ciudadanía un gran número de servicios. Estos servicios están teniendo una gran aceptación y repercusión positiva en la opinión pública, que está demandando una utilización más generalizada de la red.

La FNMT-RCM apostó por Ceres allá por el año 1996; desde entonces, su trayectoria le ha llevado a facilitar el acceso a un elevado grupo de aplicaciones que requieren la utilización de los certificados digitales, de hecho, los últimos años han sido muy positivos ya que se ha facilitado a los ciudadanos la gestión de numerosos trámites a través de Internet de una forma segura.

Así mismo, creemos que es importante reseñar el esfuerzo que están haciendo los Organismos y las

Empresas para desarrollar el mayor número de aplicaciones que faciliten las gestiones tanto administrativas como comerciales con la utilización de los nuevos factores tecnológicos que han abierto nuevos campos en las comunicaciones, con el consiguiente ahorro de tiempo y con un mínimo esfuerzo, consiguiendo así organizaciones más flexibles y eficaces.

En la actualidad, existen aproximadamente 610.000 usuarios activos de los servicios de certificación de la FNMT-RCM, distribuidos por todo el territorio nacional, que hasta la fecha han realizado decenas de millones de transacciones seguras de todo tipo sin que se haya detectado ninguna anomalía. Además, el número de usuarios no solo se duplica cada año, sino que se verá incrementado notablemente, con la aparición de nuevos aplicativos que, tanto empresas como organismos de la Administración, están comprometidos y decididos a ofrecer para mejorar su gestión y sus servicios.

Servicios con certificados digitales

Las gestiones que mediante la utilización de los certificados digitales puede Ud. hacer desde su domicilio o su empresa con Ayuntamientos como el de Madrid, son: consulta de multas de circulación, domiciliación bancaria de tributos municipales y tasas (IBI, IVTM, IAE...), consulta a colegios electorales; con el Ayuntamiento de Valencia: consulta de datos padronales, emisión de certificados de empadronamiento, consulta de todo tipo de certificados emitidos por el Ayuntamiento, consulta de facturas y su estado de trámite para proveedores, consulta de instancias y expedientes donde el ciudadano conste como interesado (movimientos, actuaciones, notificaciones, acuerdos municipales...)

La Diputación de Barcelona facilita la notificación electrónica de publicaciones y tasas así como el servicio de difusión selectiva de información.

Igualmente, las Comunidades





Autónomas han puesto a disposición de los ciudadanos servicios específicos, entre los que se puede citar a la Junta de Castilla y León, con el Registro de movimientos del ganado en su programa Simocyl y la solicitud de ayudas para la modernización de explotaciones y para forrajes desecados, así como la Oficina Virtual de Impuestos Autonómicos. La Junta de Castilla-La Mancha facilita a través de los certificados de la FNMT-RCM, el Diligenciado Automático de Certificados de Instalación Eléctrica de Baja Tensión (eDice); la Junta de Andalucía ha desarrollado además de procedimientos tributarios de la propia Junta, un variado número de procedimientos internos dirigidos a su personal, así como trámites de investigación y para las Universidades, y de Medio Ambiente para colectivos registrados. En la Comunidad de Madrid a través de los certificados se pueden realizar trámites para el alta de empresas, la gestión del juego con autoliquidación de impuestos, autorizaciones de tarjetas de transporte mediante intercambio de apuntes registrales, firmados electrónicamente, con el Ministerio de Transportes y la consulta de estado de pago a empresarios de facturas de la CAM, entre otros servicios.

Y así podemos seguir citando un gran número de servicios puestos a disposición de los ciudadanos por departamentos ministeriales, como es el caso de la Oficina Virtual del Catastro que permite, de una forma ágil y cómoda, realizar la solicitud de certificados de todos los bienes a nombre del solicitante, sin olvidarnos del gran número de transacciones que permite la AEAT con estos certificados, la posibilidad de la solicitud de patentes y el pago de tasas a la Oficina Española de Patentes y Marcas, y la firma electrónica de las disposiciones a publicar en el BOE.

La clave del éxito

Un factor clave de éxito de esta iniciativa desde sus inicios, ha sido la rápida

capacidad de adaptación y evolución de la Entidad de Certificación de la FNMT-RCM, de forma paralela a la propia evolución de las tecnologías de la Información y redes públicas, y a la continua demanda de este tipo de servicios por la sociedad prestando en la actualidad una serie de servicios que se pueden denominar "avanzados", como son el sellado de tiempo, es decir, constancia de fecha y hora en las transacciones electrónicas; los servicios de Notificación segura a ciudadanos con no repudio en destino; el Voto electrónico en Juntas Generales de Sociedades; la validación on-line de los certificados vía OCSP, lo que permite la validación de las transacciones al instante.

En línea con la evolución técnica de CERES, se han incluido en la infraestructura, sistemas de soporte a la certificación de atributos, componentes de integración con directorios externos y la infraestructura sobre la que se ofrecerán servicios de soporte a mecanismos de pago a la Administración en aplicaciones desarrolladas por Organismos.

La naturaleza de los servicios ofrecidos exige niveles de seguridad que garanticen tanto la validez legal de los servicios como la protección de los datos personales de usuarios, el papel principal de la infraestructura de la Entidad de Certificación de la FNMT-RCM exige la manipulación y almacenamiento tanto de claves como de datos personales de todos los usuarios, incluyendo por ejemplo números de identificación fiscal.

Tarjeta criptográfica

Es importante destacar que los usuarios que lo deseen pueden hacer uso de tarjetas inteligentes con criptoprocador como soporte físico de los certificados, facilitando así su interacción con la Entidad de Certificación e incrementando considerablemente el nivel de seguridad de las aplicaciones, dado que las claves secretas nunca abandonan la tarjeta, realizándose todas las operaciones criptográficas relevantes

dentro de ella.

Inciendiando en el tema de la tarjeta criptográfica se puede reseñar que la FNMT-RCM, en cumplimiento de la Ley 59/2003 y de la Decisión de la Comisión Europea de 14 de julio de 2003 (L. 175/45, 15/7/2003), fabrica y distribuye dispositivos seguros de creación y verificación de firma electrónica que soportan generación y custodia de claves en la propia tarjeta, así como la personalización que corresponda. Esta tarjeta es la única que a la fecha está siendo evaluada por la autoridad nacional competente (Centro Nacional de Inteligencia - Centro Criptológico Nacional).

La tarjeta CERES v.3.0. es capaz de soportar más de 15 certificados X.509 distintos, con independencia de la CA y presentar unas capacidades y velocidades que la sitúan en una posición de liderazgo en el ámbito internacional, su capacidad de procesamiento y su alta seguridad hacen de estas tarjetas las más apropiadas para sistemas de gestión inteligente.

Los servicios de publicación, mediante los cuales se da a los usuarios acceso a certificados o a información sobre los mismos, listas de certificados revocados, o cualquier otra información relativa a los servicios de la Entidad de Certificación incluyen la publicación de políticas y normas, poniendo a disposición de los usuarios la declaración de prácticas de certificación (CPS), un Directorio seguro de certificados y la publicación de certificados o listas de revocación por medios distintos al directorio seguro, por ejemplo dando acceso en línea a información sobre el estado de los certificados (vigente, suspendido o revocado).

Por último, comentar que el carácter universal y de servicio público, de los servicios ofrecidos por la infraestructura exige el uso de tecnologías abiertas y normalizadas, que no imponen a los usuarios finales requisitos técnicos específicos en los sistemas de acceso a los servicios. 

