LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA COMO ENTIDAD DE CERTIFICACIÓN PARA LAS ADMINISTRACIONES PÚBLICAS

1- ANTECEDENTES Y OBJETIVOS

El objetivo de la Entidad de Certificación de la FNMT–RCM es facilitar la comunicación vía Internet entre la Administración Española y sus administrados, así como las comunicaciones entre los distintos Órganos de la Administración. Esto permitirá en un futuro cercano realizar innumerables gestiones con las distintas Administraciones sin necesidad de desplazarse y con el consiguiente ahorro de tiempo y coste, permitiendo tener una Administración abierta las 24 horas del día y los siete días de la semana.

La Entidad de Certificación de la FNMT–RCM se plantea dentro de este marco con un objetivo doble: por un lado, establecer la infraestructura técnica necesaria para garantizar la seguridad en cuanto a autenticidad, integridad, confidencialidad y no repudio de las transacciones electrónicas realizadas en el ámbito administrativo entre ciudadanos y empresas con las Administraciones Públicas o de éstas entre sí; y, por otro lado, proponer la reglamentación necesaria para otorgar validez a los actos administrativos que se produzcan por esta vía.

2- EL MODELO DE CERTIFICACIÓN DE LA FNMT - RCM

Desde un punto de vista de operación, el principal requisito establecido para la infraestructura de La Entidad de Certificación de la FNMT-RCM es la transparencia al usuario: la FNMT-RCM es un intermediario transparente al ciudadano que garantiza a los partícipes de una comunicación la seguridad en términos de autenticidad, integridad, confidencialidad y no repudio de la información intercambiada.

Asimismo se han establecido las siguientes directrices generales de operación:

- disponibilidad máxima, facilidad de uso y gran capacidad de acceso concurrente;
- seguridad interna certificable según los criterios ITSEC/ITSEM, los Common Criteria con TCSEC y la normativa británica BS7799, aplicando sistemáticamente la metodología del MAP MAGERIT como herramienta de análisis y evaluación de riesgos;
- auditabilidad, siendo posible en todo momento registrar y acceder a los eventos significativos que tienen lugar en la infraestructura;

- interoperabilidad con otras infraestructuras, lo que exige adecuar el sistema a tecnologías abiertas y a las normas internacionales reconocidas como ITU-T X.509 versión 3, recomendaciones del grupo de trabajo PKIX de IETF, LDAP versión 3, ITU-T X.500, PKCS, CryptoAPI de Microsoft y CDSA;
- escalabilidad en cuanto al número de usuarios (millones) como en cuanto a la tipología de servicios a prestar. En esta línea cabe destacar que la FNMT-RCM no solamente presta los servicios típicos de una autoridad certificadora, sino que también ofrece servicios avanzados de tercera parte de confianza como sellado de tiempo, servicios de no repudio, certificación y archivo de mensajes, etc.
- adaptabilidad ante previsibles cambios tecnológicos, evolución de estándares o normativas o bien ataques exitosos a los algoritmos criptográficos utilizados.

De acuerdo con las directrices de operación anteriores, las principales características técnicas de la infraestructura de la Entidad de Certificación de la FNMT-RCM son:

- Registro distribuido, con presencia física del usuario en una oficina de Correos. Posibilidad de registrar ciudadanos, empresas, Organismos o equipos informáticos. Posibilidad de registrar representaciones.

- Pares de claves generados centralizadamente por la infraestructura. Utilización de dos pares de claves por usuario, uno orientado a autenticación y otro como soporte de confidencialidad. Las claves privadas de autenticación serán destruidas con métodos que garantizan las medidas más estrictas de seguridad (nivel E4 según los criterios ITSEC), mientras que las claves privadas de soporte de confidencialidad podrán quedar archivadas en la Entidad Pública de Certificación para los casos en que se requiera la recuperación de documentos cifrados (por ejemplo en caso de pérdida o deterioro de la tarjeta por parte del usuario).

- Tarjeta inteligente de usuario con microprocesador, con claves privadas en su interior que nunca abandonan la tarjeta, realizándose en su interior las operaciones criptográficas más relevantes y evitando copias de claves. La tarjeta ofrece funciones RSA de 1.024 bits como algoritmo de clave pública y SHA-1 para el hashing.

  El sistema operativo de la tarjeta es propietario de la FNMT, sigue las especificaciones PC/SC y ofrece a las aplicaciones interfaz PKCS#11, si bien está previsto ofrecer interfaz CryptoAPI si así lo demandan las aplicaciones de usuario.

  La utilización de la tarjeta es muy sencilla para el usuario, ya que el ordenador o dispositivo de acceso la solicita cuando se desee realizar un trámite que requiera

validez administrativa. La protección de acceso a la tarjeta se realiza mediante PIN, aunque también se están considerando protecciones biométricas de cara al futuro. El PIN o palabra de acceso será conocida únicamente por el propio usuario, encargándose el sistema informático del Organismo, junto con la infraestructura de la FNMT, de realizar el resto.

Esta tarjeta es la que servirá como "DNI cibernético" en las operaciones en la red, garantizando la identidad del usuario, la del interlocutor así como la integridad y confidencialidad de la información transmitida.

- Emisión de certificados en línea, lo que garantiza que el certificado de clave pública se emite únicamente cuando el usuario demuestra posesión de la clave privada correspondiente. Con este propósito se entrega personalmente al usuario en el momento del registro una clave numérica que le permite activar la tarjeta y acceder en línea a La Entidad de Certificación de la FNMT-RCM, que entonces emite su certificado.

- Directorio seguro con servicio de consulta on-line del estado del certificado, accesible vía LDAP o X.500-DAP pero que también permitirá consultar certificados o listas de revocación vía protocolos como OSCP cuando estos se implanten.

- Acceso a los servicios de la Entidad de Certificación de la FNMT-RCM a través de redes públicas (Internet, RedIP), redes de valor añadido o específicas de la Administración (como ISTMO o RICO), con protocolo de transporte TCP/IP.

- Soporte de todo tipo de aplicaciones de usuario mediante interfaces abiertos y normalizados, incluyendo aplicaciones basadas en web, sistemas de mensajería, sistemas de seguridad de acceso en redes privadas virtuales (por ejemplo basadas en Ipsec), sistemas EDI, etc.

3- MEDIOS UTILIZADOS

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.

En un primer momento se configuró una infraestructura técnica a pequeña escala orientada al desarrollo, integración y prueba de componentes técnicos para la infraestructura definitiva, así como a servir de soporte y prueba de concepto al desarrollo de aplicaciones piloto por parte de Organismos.

La infraestructura se basaba en un pequeño número de LANs interconectadas a través de un firewall, cada una de ellas con varios puestos de desarrollo y pequeños servidores de grupo de trabajo gestionados independientemente; los procesos criptográficos se llevaban a cabo en software y existía a través del firewall conectividad con redes externas a través de un router. Servicios como el de correo electrónico o web público se apoyaban en la infraestructura Intranet ya existente en la F.N.M.T.

Esta infraestructura inicial dio paso a la arquitectura actual más evolucionada, que se compone de diversos entornos de desarrollo y tres entornos productivos para las diferentes clases de servicio que ofrece la infraestructura (Pilotos, Clase 1 y Clase 2). Existen recintos separados y sistemas de vigilancia y control de acceso físico a los diferentes recintos. Disponemos asimismo de diferentes sistemas firewall (algunos configurados en alta disponibilidad) para el control de tráfico entre los diferentes entornos y acceso a redes externas a través de accesos Frame-Relay, RDSI y líneas dedicadas.

En cada uno de los entornos productivos se dispone de equipos servidores de alto rendimiento y fiabilidad, con sistemas de alimentación, almacenamiento y procesadores redundantes. Los procesos criptográficos se llevan a cabo en hardware dedicado de alta seguridad, certificados según FIPS 140-1 nivel 3. Los sistemas operativos en producción están certificados al menos a nivel E3/F-C2 según ITSEC. Desde esta infraestructura se ofrecen también los servicios de web y correo electrónico externo, tanto para la propia infraestructura de la Entidad de Certificación de la FNMT-RCM como para la F.N.M.T.

En línea con la evolución técnica del proyecto, los principales desarrollos previstos a corto y medio plazo en la infraestructura incluyen sistemas de soporte a la certificación de atributos, componentes de integración con directorios externos y la infraestructura sobre la que se ofrecerán servicios avanzados, como el fechado digital o los servicios de soporte a mecanismos de pago a la Administración en aplicaciones desarrolladas por Organismos. Se sigue, asimismo, una línea de migración gradual de la infraestructura incrementando su capacidad transaccional (para garantizar la escalabilidad del servicio a millones de usuarios), tolerancia a fallos (incorporando entornos remotos redundantes), y seguridad.

Los requerimientos de personal para la operación de los diversos entornos productivos, así como para el soporte a usuarios, desarrollo de nuevos servicios e implantación de nuevos componentes de la infraestructura técnica, han evolucionado de igual manera. En estos momentos el proyecto dispone de más de 60 personas trabajando en las distintas áreas en que se divide, con más de 20 personas dedicadas a nuevos desarrollos y proyectos de investigación en áreas como el fechado digital, certificación cruzada para garantizar la

interoperabilidad con otras infraestructuras nacionales e internacionales, certificación de atributos, o sistemas de pago a la Administración, y existen planes a corto plazo para incorporar 30 personas más.

4- SITUACIÓN ACTUAL DEL PROYECTO

Desde el punto de vista legal, el Gobierno español ha aprobado recientemente:

- Real Decreto 1290/1999, de 23 de Julio, por el que se desarrolla el Art.81 de la Ley 66/1997.

- Real Decreto-Ley 14/1999, de 17 de Septiembre, sobre Firma Electrónica.

- Ley 55/1999, de 29 de Diciembre, de Medidas Fiscales, Administrativas y del Orden Social. En su Art.51 se modifica el Art.81 de la Ley 66/1997, de 30 de Diciembre, de Medidas Fiscales, Administrativas y del Orden Social, adicionando dos nuevos apartados en los que se amplía la prestación de los servicios de la FNMT-RCM, como Entidad de Certificación a los Órganos Jurisdiccionales.

Por otra parte, desde el punto de vista técnico, la infraestructura ya se encuentra operativa, con un número importante de Organismos en fase de desarrollo y prueba de sus aplicaciones de servicio público a prestar a través de Internet. En paralelo también estamos desarrollando trabajos técnicos con la infraestructura extendida, esperando que pueda estar disponible para su despliegue durante los próximos meses.

De igual manera la F.N.M.T. está desarrollando una Autoridad de Fechado digital que pretende ofrecer servicios de sellado de tiempo no sólo a la Entidad de Certificación de la FNMT-RCM sino a otras Autoridades de Certificación que no gocen de este tipo de servicio. Esta iniciativa supone la continuación de carácter práctico del proyecto de “Sellado de tiempo” que la Unión Europea adjudicó a la FNMT en consorcio con Correos y el Ministerio para las Administraciones Públicas para la definición de un modelo europeo de certificación temporal.

En cuanto a Organismos usuarios de la infraestructura cabe destacar la AEAT y numerosos Departamentos de la Administración General del Estado (MAP, Ministerio de la Presidencia, Ministerio de Agricultura, Ministerio de Justicia, etc.), de Comunidades Autónomas (Junta de Galicia, Baleares, Canarias, Madrid, Castilla y León, etc.), de Ayuntamientos y otras Entidades Locales (Ayuntamiento de

Sabadell, Madrid, Zaragoza, etc.), Diputaciones, así como Universidades y Colegios Profesionales.

En el año 1999 y 2000 se han realizado dos importantes aplicaciones: el pago del impuesto de la renta y del IVA, y las retenciones a cuenta para las PYMES. Hasta la fecha se han emitido unos 55.993 certificados y se han presentado alrededor de 136.803 declaraciones a través de Internet. La iniciativa ha superado con creces las expectativas y metas que nos habíamos fijado al inicio de la campaña. Se han solicitado certificados y presentado declaraciones desde prácticamente todos los puntos de España, así como desde los más diversos colectivos.

También se ha estado trabajando con todos los fabricantes del Euro para securizar el correo electrónico, medio utilizado para el envío de información confidencial sobre la nueva moneda.

Otro de los objetivos ha sido establecer acuerdos de interoperabilidad para poder ofrecer certificación cruzada con otros proveedores de certificación similares a la Fábrica de la Moneda que surjan en otros países, de forma que nuestras empresas y nuestros ciudadanos puedan contactar a través de una vía segura con ciudadanos y empresas de otros países del entorno de la Unión Europea o del exterior de la misma. Cabe destacar el convenio firmado con una empresa alemana que realiza un proyecto similar al que se está realizando en España, de ámbito también público. Se han establecido conversaciones con el Reino Unido y con los Estados Unidos con el fin de realizar certificación cruzada entre estos países.

5- CONCLUSIONES

Las oportunidades que la Entidad de Certificación de la FNMT-RCM ofrece a las distintas Administraciones para prestar sus servicios públicos a través de Internet con garantías legales y de seguridad son enormes: pago de impuestos, solicitud y gestión de certificados, renovación de documentos, presentación de reclamaciones y un sinfín de trámites administrativos tanto internos como con ciudadanos y empresas.

También se perciben grandes ventajas desde el punto de vista del ciudadano como ahorros de costes y desplazamientos, comodidad, reducción de plazos de tramitación, etc., ya que la ventanilla única de acceso a la Administración pasará a ser el PC o la televisión, a cualquier hora del día o de la noche, sábados y domingos incluidos.

A través de iniciativas como la Entidad de Certificación de la FNMT-RCM, el e-government en España empieza a ser una realidad.