

Izaskun Loinaz.-
La Dirección General de Tráfico ha implantado una Infraestructura de Clave Pública (PKI) interna para la emisión de certificados digitales. Esta infraestructura le permite automatizar el intercambio de información con las mayores garantías de seguridad, utilizando los servicios de firma electrónica y cifrado basada en certificados digitales. Por ello, la DGT está planificando la ampliación del sistema a otros organismos públicos y privados con los que mantiene comunicaciones habitualmente, como son los ayuntamientos.

La solución, operativa desde diciembre de 2002, va a someterse a una modificación y ampliación del software, que permita automatizar aspectos que hasta el momento complicaban el nivel de explotación.

Durante años la Dirección General de Tráfico (DGT) dispuso de varias aplicaciones que utilizaban un sistema de correo electrónico seguro con certificados digitales que les permitía agilizar sus procesos administrativos. Sin embargo se considera conveniente la adopción de una PKI interna puesto que los certificados digitales utilizados en estas experiencias provenían de productos cuya utilización y gestión no les permitía extender su uso. De esta manera, la entidad ha conseguido automatizar la recepción de la información con las mayores garantías de seguridad.

El proyecto de implantación de la solución del Grupo SIA –en el que se han invertido hasta el momento aproximadamente unos 90.000 euros– comenzó en otoño de 2002 y se finalizó en diciembre de ese mismo año. Fueron casi tres meses en los que se llevó a cabo el análisis, implantación e integración con el directorio que había en la DGT. La solución está operativa desde diciembre de 2002 y actualmente se está realizando una modificación y ampliación del software, que permitirá optimizar las tareas de explotación del sistema y ampliar su alcance a un mayor número de organizaciones. Sin embargo, después de detectar diversos problemas de rendimiento en equipos antiguos (con Windows 98), la DGT decidió actualizar su parque de puestos con la adquisición de 1.300 nuevos equipos dotados con las últimas tecnologías, como lector de tarjeta inteligente incorporado en el teclado.

Como explica Javier Guerrero, jefe de Servicios de Sistemas Informáticos de la Dirección General de Tráfico, ya en el año 2001 surge la necesidad de intercambio de una serie de ficheros. El primero de ellos, se trataba del fichero FiVA (Fichero de Vehículos Asegurados), donde se automatizan y se recogen los datos relativos a seguros de automóviles, ciclomotores, etc., intercambiado con el Consorcio de Compensación de Seguros y amparado bajo la Ley de Protección de Datos. Así, se plantea la necesidad de realizar un intercambio de datos vía *email* en el que la DGT procese el fichero y automáticamente responda si el proceso ha sido correcto o se han producido errores. “Al decidir hacerlo por esta vía nos topamos con la necesidad de enviar esos datos cifrados y firmados, como manda la ley. La única herramienta que encontramos para ello en ese momento fue OpenSSL, una *opensource* basada en el sistema operativo Linux, con la que empezamos a emitir nuestros certificados para organismos externos”, asegura Guerrero.



Fotos: Jesús Mirón

Javier Guerrero, jefe de Servicios de Sistemas Informáticos de la Dirección General de Tráfico

En esta primera fase, además de al Consorcio de Compensación y Seguros se incluyó al Registro General de Bienes y Muebles, que les remite información sobre el estado de los vehículos. Pero, según Javier Guerrero, “se nos plantean nuevas necesidades desde ayuntamientos, autoescuelas, inspecciones de vehículos, etc., en cuanto a la mejora del intercambio de información con ellos, y automatización de los procesos, basándolos en herramientas que aporten seguridad. Por ello, decidimos implantar una herramienta basada en OpenSSL, en modo texto, no gráfico, y que no permite un control basado en servicios de directorio”.

Finalizada la primera fase, en el 2002 se decide implantar los servicios de directorio de la DGT. Para ello se basan en las soluciones de Directorio Corporativo de iPlanet. De esta manera, su primer uso es como repositorio de información de todos los funcionarios de la Dirección General de Tráfico y lo extienden para adoptar una plataforma de PKI. Poco después surge la necesidad de adquirir de manera rápida una plataforma de PKI que sirva para los propósitos que la DGT destina a los servicios de intranet o Internet bajo una seguridad basada en certifica-

INVIERTE EN LA IMPLANTACIÓN DE LA PLATAFORMA PKI DEL GRUPO SIA

La DGT automatiza el intercambio de datos

dos digitales. Para ello se analizaron y realizaron pruebas de diferentes productos PKI entre los que se encontraban los propuestos por el Grupo SIA, adquiridos posteriormente a través del catálogo de Patrimonio. Entre sus puntos fuertes está la integración con el servicio directorio donde se almacenan las listas de revocados y desde donde se expiden con la Autoridad de Registros, con los certificados tanto para funcionarios de la DGT como para organismos externos. El proyecto fue presentado en la Comisión Ministerial de Informática en noviembre de 2002 cuando Ana Pastor, actual ministra de Sanidad y antigua subsecretaria del Ministerio del Interior, decide que el Ministerio de Interior tiene que llevar la plataforma PKI a todos sus funcionarios. "Decidimos montar el piloto con SIA y dar a todos los directivos de la DGT una certificación electrónica basada en soportes seguros", indica Guerrero.

Tras las pruebas iniciales, se emiten las primeras 100 tarjetas inteligentes que almacenan los certificados de la DGT y se decide ampliar el despliegue a todos los funcionarios de la DGT que dispongan de correo electrónico seguro, utilizando certificados digitales almacenados en tarjeta o en software

Ante la necesidad de automatizar el intercambio de correo electrónico con todos los organismos externos, la DGT solicita a SIA, dentro de la contratación de la PKI, la elaboración de una aplicación software para lograr este objetivo. Para ello se elaboró un programa desarrollado en Java en producción desde diciembre de 2002. "Actualmente estamos en fase de una modificación de dicho software que nos permita automatizar aún más el número de organismos externos que puedan comunicarse con la Dirección General de Tráfico, como son los centros de ITV y autoescuelas, estas últimas elegidas como piloto debido al gran universo que representan. Más tarde, una vez superada esta fase, se procederá a implantar esta misma solución para la comunicación con los ayuntamientos de toda España.

Un aspecto importante de la solución PKI que ha adoptado la DGT es que puede emitir con la misma infraestructura certificados tanto en soporte tarjeta, soporte software, como para redes privadas virtuales, es decir, en la misma infraestructura se emiten certificados para usuarios en varios formatos y para diferentes equipos como WebServers, routers, etc.

El proceso de transformación lo describe Guerrero con la siguiente frase: "en dos años hemos pasado de no tener plataforma de correo electrónico a intercambiar datos de forma automática y segura basada en certificados digitales. Además, hemos tenido la posibilidad de, a través de los servicios directorio, extender todos estos pilotos completamente a cualquier organismo que esté autorizado a intercambiar datos con nosotros de manera versátil y escalable. Desde la implantación del correo electrónico seguro, hemos observado que la gente ha aceptado el cambio perfectamente sin que se haya producido ningún impacto".

PLATAFORMA PKI IMPLANTADA POR EL GRUPO SIA

PKI-CA/RA	Entrust Authority / Security Manager
Certificados Usuario	Entrust Enrollment Server for Web Certificados X.509v3 por SSL y S/MIME
Certificados VPN	Entrust Enrollment Server for VPN Certificados X.509v3 para Routers IPSec
Directorio	Integración con directorio iPlanet existente en la DGT
Tarjetas Inteligentes	Tarjetas criptográficas Gemplus con lectores PC/SC
Aplicación, Automatización y Seguridad en e-Mail	Aplicación Java desarrollada por SIA para automatización en la recepción de correos firmados y cifrados

Todos los productos y las aplicaciones internas de seguridad se han basado en los estándares más conocidos. De esta forma, toda la infraestructura de la DGT puede reconocer certificados de cualquier entidad tanto pública como privada siempre que cumpla los estándares.

En este sentido, Guerrero insiste en que no están "casados con ninguna entidad certificadora, con ningún software específico". "Estamos en fase de evaluación, la PKI satisface completamente nuestras necesidades, pero no se descarta poder evaluar o decidir en el futuro tener otros productos de certificación", añade.

Tal y como explica Guerrero, en la actualidad se encuentran en plena fase de análisis de herramientas que les permitan, a partir de la PKI, automatizar la gestión de usuarios de la DGT, con el fin de automatizar y controlar el acceso de todas sus aplicaciones. Asimismo, existe un proyecto piloto con el Banco Santander Central Hispano que se implantará durante este año y que permitirá pagar directamente las sanciones a través de todas las sucursales de dicha entidad.



de forma segura