

TGSS: servicios de certificación para usuarios del sistema RED

La Subdirección General de Informática de la Tesorería General de la Seguridad Social (TGSS) ha acometido un importante proyecto de mejora de la infraestructura de seguridad y nivel de servicio en el sistema RED (Remisión Electrónica de Documentos) para el que ha confiado en la experiencia del Grupo SIA como integrador de sistemas y consultor tecnológico especializado en seguridad. Se ha utilizado la tecnología Entrust, tanto como PKI como para autorizaciones (PMI). El proyecto ha sido dirigido por el Centro de Calidad, Auditoría y Seguridad, y consiste en la implantación de una Plataforma de Certificación Electrónica que puede emplear certificados de múltiples Autoridades de Certificación.



Raúl Olivar

El sistema RED es un servicio que proporciona la Tesorería General de la Seguridad Social a empresas, profesionales y gestores, cuya finalidad es realizar gestiones directas con la TGSS, permitiendo el intercambio seguro de información y documentos entre este organismo público y los usuarios a través de Internet.

Como parte del proyecto, la TGSS ha implantado su propia PKI para emitir certificados a los usuarios del sistema RED, lo cual le permite ofrecer un mejor nivel de servicio, dotándoles de todas las capacidades de firma digital y cifrado de una manera sencilla.

El proyecto incluye igualmente la migración transparente de la situación anterior, basada en certificados de terceros, así como la utilización directa del navegador, eliminándose así la necesidad de disponer de un *software* cliente PKI en el puesto de los usuarios. El alcance actual se cifra en 100.000 usuarios, que acceden directamente desde el portal de la Seguridad Social (www.seg-social.es).

TRANSFERENCIA DE INFORMACIÓN SEGURA CON LA TGSS A TRAVÉS DE INTERNET: EL SISTEMA RED (Remisión Electrónica de Documentos)

El sistema RED es un servicio que proporciona la TGSS a empresas, profesionales y gestores, cuya finalidad es realizar gestiones directas con la TGSS, permitiendo el intercambio seguro de información y documentos entre este organismo público y los usuarios a través de Internet. RED permite el acceso al sistema

de la TGSS para consultar y modificar los datos de una empresa y de sus trabajadores, así como la posibilidad del envío de documentos de cotización, afiliación y partes de alta y baja en el Instituto Nacional de la Seguridad Social (INSS). Este sistema permite, además, agilizar la relación entre la Seguridad Social y las diferentes empresas y despachos, eliminando así el circuito del papel con una importante mejora en la calidad de los datos, evitando largas esperas en las oficinas de la Administración. Previamente a la implantación de esta nueva infraestructura el sistema RED funcionaba vía X-400 o vía Internet con certificados de la FNMT-RCM y *software* cliente instalado en el PC del usuario.

Actualmente el sistema RED representa del orden del 85%

del trabajo de afiliación y el 90% en la parte de cotización de la Seguridad Social.

Los principales motivos que llevaron a la TGSS a plantearse la migración al nuevo sistema fueron básicamente las dificultades del sistema anterior en cuanto a escalabilidad, nivel de servicio, necesidad de distribución de *software* con sus incidencias asociadas y la deficiencia de capacidades de administración y control sobre las operaciones de gestión de los certificados de usuarios. Para solventar estos problemas, el Grupo SIA presentó un proyecto basado principalmente en la eliminación del *software* cliente en el PC del usuario final y la implantación de una Autoridad de Certificación que permitiese a la TGSS emitir certificados para sus usuarios internos y controlar a la vez el alto nivel de servicio que requieren sus aplicaciones de negocio, como es el caso del sistema RED.

OBJETIVOS DEL PROYECTO

El principal objetivo perseguido por la TGSS con la migración de las infraestructuras de seguridad del RED hacia el nuevo sistema, es la garantía de un alto nivel de servicio y una baja tasa de incidencias. Además, el sistema debe ser capaz de trabajar con múltiples autoridades de certificación, ser totalmen-

La TGSS y el Sistema RED

La magnitud de los datos de la Seguridad Social, hacen actualmente del sistema RED y sus tecnologías uno de los mayores y más avanzados proyectos de administración electrónica no solo de nuestro país sino también a nivel europeo.

La Subdirección General de Informática de la TGSS gestiona más de 16 millones de trabajadores, 8 millones de pensionistas y 2 millones de empresas, con 20.000 puntos de acceso de gestores propios, externos y terminales automáticos y más de 1.200 oficinas de la TGSS, INSS, ISM, INSALUD, IMSERSO e Intervención. Mensualmente se procesan más de 4 millones de accesos por Internet del sistema RED.

te transparente para los usuarios nuevos y existentes, fácil de usar y absolutamente escalable. Todo ello con la máxima flexibilidad en el despliegue, y la garantía de la imagen y el nivel de servicio de la TGSS, y el mantenimiento de altos niveles de seguridad gestionada en la autenticación, firma y cifrado de la información tramitada.

Otras metas buscadas en el proyecto son:

- Mantener las mismas funcionalidades sin el uso de *software* instalado en el PC del usuario, eliminando toda necesidad de distribución de *software* a los clientes finales.

- Permitir que los usuarios actuales del sistema puedan interactuar con la nueva infraestructura sin necesidad de realizar ningún cambio en su PC.

- Ser flexible y trabajar con múltiples Autoridades de Certificación de confianza en las operaciones de autenticación y firma digital de una forma transparente para los usuarios. (Estas Autoridades de Certificación no se han determinado aún, pero se ha prestado especial importancia la posible relación con el despliegue del DNI electrónico).

- Disponibilidad de los mecanismos necesarios para la recuperación de las claves de descifrado, en caso de necesidad, de una manera transparente para el usuario.

La infraestructura de PKI interna se ha dimensionado inicialmente para 100.000 usuarios internos.

FUNCIONALIDAD DEL SISTEMA

La parte funcional más importante del sistema RED es la relacionada con las aplicaciones que posibilitan al usuario un contacto cotidiano con la TGSS. En este apartado se hará hincapié solamente en las relacionadas con la nueva infraestructura instalada, ob-

jeto de este artículo.

Los usuarios disponen así de un sistema integrado de autenticación y autorizaciones según su perfil, proporcionados respectivamente por la PKI y por la infraestructura de gestión de privilegios (PMI). De este modo, se tienen las operaciones de registro de nuevos usuarios, canje de los certificados Clase 1S de la FNMT, acceso en línea al sistema y envío de ficheros.

Registro

Es el primer paso de toda nueva persona o entidad que desee incorporarse al RED e

desde la Intranet de la Seguridad Social con los mecanismos de seguridad propios de esta arquitectura que permiten en línea las siguientes operaciones:

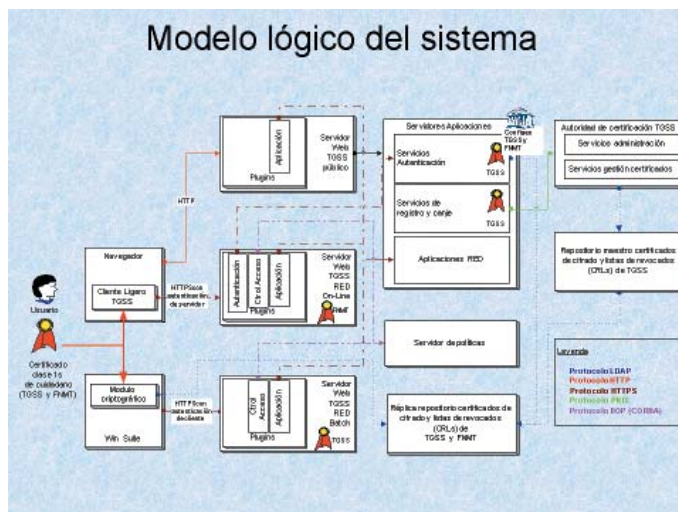
- Creación y recuperación de certificados para personas.

- Creación y recuperación de certificados para máquinas.

- Revocación de los certificados emitidos para una persona o máquina.

- Desactivación y activación de un usuario.

- Recuperación de datos y estadísticas de todos los certificados de usuario.



interactuar con la TGSS a través de Internet. Con él se consigue un certificado, llamado certificado SILCON dentro del ámbito del proyecto, que permite al usuario garantizar su identidad, la confidencialidad de las comunicaciones y los datos, así como su integridad y el no repudio de las transacciones realizadas.

La solicitud del certificado se realiza en las Unidades de Atención al Usuario (UAU) de las Direcciones Provinciales de la TGSS. El proceso de registro es presencial y en él el usuario debe acreditar su identidad mediante su DNI o pasaporte.

Técnicamente el registro es un servicio web accesible a los registradores de las UAUs

Canje

Los usuarios actuales, que ya disponen del certificado digital clase 1S CA (dos pares de claves para firma y cifrado almacenado en software) de la FNMT, no precisan acudir a las oficinas de registro para obtener su certificado SILCON, pueden canjearlo directamente a través de Internet. Para ello solamente deberán utilizar la opción habilitada para tal fin en la página www.seg-social.es

Técnicamente, el canje es un servicio web accesible a todos los actuales usuarios a través de Internet autenticado mediante certificado FNMT que proporciona, tras firmar

digitalmente un contrato de aceptación, un certificado SILCON emitido por el nuevo servidor de gestión de certificados digitales de la Seguridad Social a partir de los datos contenidos en el certificado original de la FNMT.

Acceso en línea

El usuario dispone de dos modalidades de acceso con el sistema: el acceso en línea y el envío de ficheros para su proceso en *batch*. En la web hay disponibles múltiples opciones para consulta y actualización de información.

Técnicamente el acceso en línea se realiza mediante un servicio web, protegido con SSL con autenticación de servidor, donde la navegación se ejecuta a través de menús personalizados. La autenticación está basada en la firma digital realizada por el usuario, con las claves privadas y su perfil o alguna CA confiable almacenados en su PC mediante un software descargado en tiempo de ejecución (*applet*). Este último también ofrece posibilidades de firma de formularios y transacciones así como de cifrado de información. Esta autenticación está integrada con la herramienta de control de accesos, que personaliza la navegación y discrimina las operaciones y transacciones en función de los roles del usuario asociados a su perfil.

Este sistema permite la movilidad total del usuario al no requerir ninguna instalación especial en su equipo de trabajo. Solo es necesario su perfil, una conexión a Internet y un navegador que admita *cookies* de sesión y permita la ejecución de *applets*.

Envío de ficheros

Para las empresas o usuarios que manejan grandes volúmenes de datos existe un mecanismo alternativo de actualización de información

basado en el envío de ficheros con remesas de operaciones.

Técnicamente el envío de remesas es un servicio web, protegido con SSL con autenticación de cliente, al que se accede mediante una herramienta cliente desarrollada por la TGSS llamada *WinSuite*. Esta herramienta consta de módulos de firma y cifrado de ficheros y de comunicaciones, capaz de establecer la sesión segura autenticando al cliente con el mismo perfil en *software* que se utiliza para el acceso en línea. Los permisos de ejecución de las transacciones también están supervisados por la herramienta de control de accesos.

SOLUCIÓN TÉCNICA

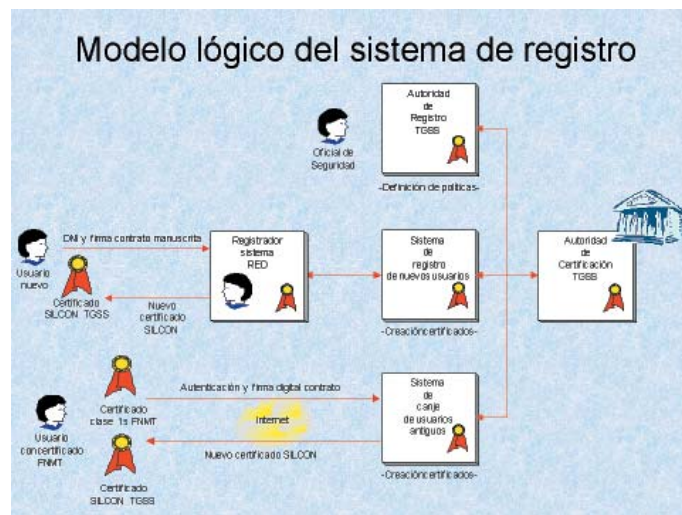
El Grupo SIA ha participado en todas las fases del proyecto, desde la definición inicial de la solución tecnológica avanzada, hasta su puesta en producción y posterior explotación, realizando tareas de consultoría, diseños, definición de documentos de prácticas y políticas de certificación (CPS y CP), desarrollos de integración, despliegues, exhaustivas baterías de pruebas y formación de administradores y usuarios. Las tecnologías base utilizadas son tecnologías abiertas y cumplen con los estándares establecidos, habiéndose seleccionado **Entrust** como PKI y PMI, y **Critical Path** como directorio LDAP X.500.

El planteamiento inicial sobre el que se ha basado todo el sistema ha sido la creación de una infraestructura que permita a los usuarios la autenticación con cualquier certificado digital emitido por una Autoridad de Certificación confiable y el cifrado de información, disponiendo de *backup* de claves de descifrado gestionado por un servidor de gestión de certificados digitales propio que garanti-

ce la disponibilidad de las mismas en caso necesario.

Todo ello junto con la necesidad ya expresada de autenticación fuerte al web, firma digital en cliente, cifrado de información y control de acceso por perfiles, ha llevado al diseño de una solución basada en los siguientes nuevos componentes:

- **Servidor de gestión de certificados digitales.** Es el componente central de la arquitectura y es el encargado de la emisión de los certificados del sistema, las listas de certificados revocados (CRLs)



y autoridades revocadas (ARLs) y publicación de esta información en el directorio. Gestiona el *backup* y recupera las claves de cifrado, además de proporcionar la renovación automática y transparente de los certificados de usuario.

- **Autoridades de registro.** Son las herramientas de administración de la CA. Permiten tanto la definición de políticas de seguridad y roles como la creación de usuarios. Esta última se realiza a tres niveles: usuarios administradores, creados en una RA central, usuarios nuevos del sistema, creados en los puntos de registro distribuidos y usuarios antiguos del sistema, creados por un proceso en línea. La autenticación para el uso de cualquiera de estas

herramientas está basada en certificados digitales.

- **Directorio.** Es el repositorio público de información de la CA. En él se publican los certificados de cifrado de todos los usuarios, las CRLs y ARLs.

- **Cliente ligero web.** Es el componente de autenticación fuerte del sistema, que además permite la firma digital de mensajes y transacciones y el cifrado de información para terceros. No requiere ninguna instalación de software en el lado cliente. Este elemento consta de

de políticas donde se definen todas las relaciones usuario-rol-recurso.

Uno de los principales objetivos perseguidos es mantener la disponibilidad total del sistema las 24 horas al día de los 365 días del año, por lo que se han incluido en la arquitectura componentes duplicados con tolerancia a fallos y/o balanceo de carga.

FACTORES DE ÉXITO

Como todo proyecto que involucra a grupos heterogéneos de trabajo procedentes de diferentes organizaciones, la definición clara de los objetivos, las tareas y responsabilidades ha sido crucial para su culminación con éxito.

La calidad de las tecnologías de vanguardia utilizadas son la base del sistema, pero muy importante también ha sido el uso de una metodología de trabajo ofrecida por el Grupo SIA, para el seguimiento a los diferentes niveles de grupos técnicos, comité técnico y comité ejecutivo formados conjuntamente por personal de la TGSS y SIA. Ello ha permitido identificar los riesgos y tomar las mejores decisiones en cada momento.

Estos aspectos han sido necesarios, pero indiscutiblemente los factores determinantes para la buena conclusión del proyecto han sido la motivación, ganas de trabajar y disposición de las personas involucradas en el mismo, cuyas acciones han culminado en la puesta en producción de uno de los proyectos más vanguardistas de administración electrónica. ■

RAÚL OLIVAR
Responsable Técnico
del Área de Infraestructuras
de Seguridad
Grupo SIA
rolivar@sia.es