

## Delt@: declaración electrónica de trabajadores @ccidentados

El Ministerio de Trabajo y Asuntos Sociales seleccionó a finales de 2001 al Grupo SIA para el desarrollo del Sistema Delt@ para la Declaración Electrónica de Trabajadores Accidentados. Según regula la Orden TAS/2926/2002, de 19 de noviembre de 2002, el sistema está operativo desde el uno de enero de 2003 y es accesible a través de la URL [www.delta.mtas.es](http://www.delta.mtas.es) para la declaración electrónica de accidentes de trabajo por parte de las empresas españolas y para los demás agentes previstos (Entidades Gestoras, Mutuas, Empresas Colaboradoras, Autoridades Laborales y Ministerio de Trabajo y Asuntos Sociales).



Manuel Villaverde López

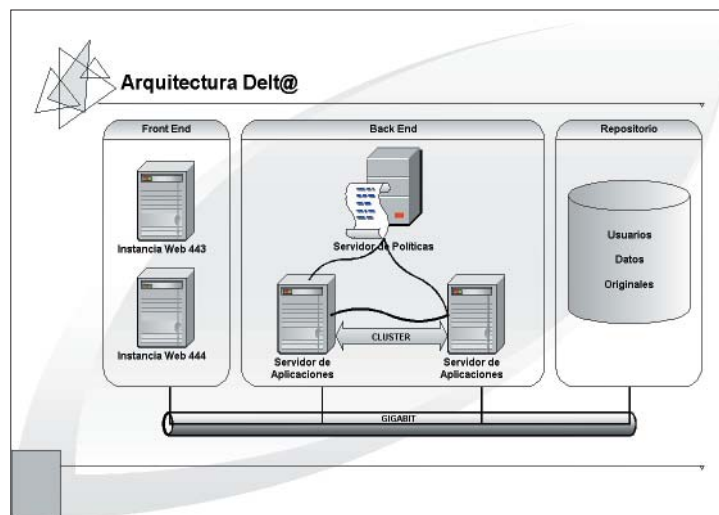
Delt@ se define como un sistema global de gestión para la notificación y tramitación de accidentes de trabajo, que incorpora las nuevas tecnologías de la información y de las comunicaciones. Dicha infraestructura está dirigida a empresas y trabajadores por cuenta propia, Entidades Gestoras (Instituto Nacional de la Seguridad Social, Instituto Social de la Marina), Entidades Colaboradoras (Mutuas y Empresas Colaboradoras), Autoridades Laborales, Subdirección General de Estadística del MTAS e Inspecciones Provinciales de Trabajo y Seguridad Social entre los que se pretende agilizar el proceso de distribución de la información, eliminando costes de grabación y depuración previa de datos, todo ello integrado con un sistema de seguridad que permita la autenticación de usuarios,

la autorización de acceso de los mismos según perfil (cada usuario podrá tener distintos perfiles dentro de la aplicación) y la confidencialidad, integridad y no repudio de la información transmitida.

Con este proyecto se avanza de manera continua hacia la administración electrónica, dando respuesta a las demandas de los ciudadanos en materia de servicio público. Se pretende conseguir una verdadera e-Administración en la que ciudadanos, empresas e instituciones tengan accesibles y a su alcance servicios públicos en línea para poder relacionarse desde cualquier lugar, a cualquier hora del día y en cualquier día de año de manera sencilla y transparente.

El proyecto Delt@ ha supuesto el diseño e implantación de una plataforma tecnológica en la que se han integrado

distintos elementos tanto hardware como software, no sólo para llevar a cabo la gestión de la información, sino también y sobre todo mucho más importante, para garantizar que dicha gestión se realiza de una forma segura.



### Tecnología de vanguardia

Los procesos y la infraestructura están especialmente desarrollados bajo estrictos niveles de seguridad. La implantación de la plataforma, desarrollada por el Grupo SIA, se ha llevado a cabo en un entorno de *housing* proporcionado por el TIC de Telefónica Data con administración remota vía VPN (sobre IPSec), sobre una máquina Unisys ES7000 con Windows 2000 Advanced Server, servidor web iPlanet, Bea Weblogic Server como servidor de aplicaciones, Bea Weblogic Integration como gestor de *workflow* y apoyándose en una base de datos Oracle 8i.

Desde el punto de vista físico, la arquitectura está organizada en tres niveles: los servicios de *front-end*, que proveen y

permiten el acceso a los usuarios; los servicios de *back-end*, que proporcionan el soporte para la lógica de la aplicación y política de acceso, y, por último, el repositorio sobre el cual se apoya todo el almacenamiento de datos.

Gracias a la escalabilidad de la plataforma hardware elegida, cada uno de los servicios se ha implantando en particiones distintas de la misma interconectadas por una red Gigabit Ethernet, para tener un mayor aprovechamiento de los recursos y un mejor rendimiento. En una primera partición de acceso descansan los servicios de *front-end*, formados por dos instancias del servidor web que son el punto de entrada al sistema y cuyas funciones son dos:

- Realizar la autenticación con el usuario, recogiendo la información del certificado del usuario y comunicándose con el servidor de políticas.

- Recoger las peticiones de los usuarios autenticados y transmitirlos a los servidores de aplicaciones para su proceso.

En otras dos particiones descansan los servicios de *back-end*, donde se dispone de un servidor de políticas y un *cluster* de los servidores de aplicaciones. El servidor de políticas es el componente en el que se concentra la lógica de autenticación del sistema. Es el que realiza la verificación de las credenciales que presenta el usuario, y en base a ellas, realiza la autenticación y asigna los privilegios correspondientes. El *cluster*, formado por dos instancias del servidor de aplicaciones, sobre el que se despliega la lógica del negocio, gestiona los diferentes flujos de trabajo.

Y en una última partición descansa el almacenamiento, caracterizado por utilizar cuatro esquemas de almacenamiento distintos: autenticación, datos, *workflow* y *log*.

### Seguridad en Delt@

En primer lugar, conviene destacar que para el acceso al sistema es necesario disponer de una certificación X.509 v.3 expedida por cualquiera de las autoridades certificadoras admitidas por el sistema, ya que la solución técnica se integra perfectamente con la infraestructura de certificados digitales proporcionados por la FNMT-RCM o cualquier otra autoridad de certificación que utilice los estándares al respecto, aunque inicialmente el sistema se apoya en certificados emitidos por

la FNMT-RCM del tipo clase 2 CA sobre tecnología Entrust. Estos certificados, almacenados en la base de datos de seguridad del navegador o en el cliente de correo electrónico, serán usados en el sistema, tanto para la firma y cifrado de datos y correo seguro como para el establecimiento de canales SSL en la comunicación web.

En cuanto a la protección de datos, según la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), se puede clasificar la información tratada en el sistema como ficheros de nivel alto, que son aquellos que contienen datos sobre ideología, religión, creencias, origen racial, salud, vida sexual, o recabados para fines policiales sin consentimiento de las personas afectadas. Esta clasificación implica que toda la transmisión de datos de carácter personal a través de las redes de comunicaciones se debe realizar cifrando los datos o usando mecanismos que garanticen que la información no es inteligible ni manipulada por terceros. En este sentido, Delt@ integra mecanismos de conexión segura, el uso de certificados digitales para la autenticación entre cliente y servidor, cifrado de datos y firma digital, los cuales se detallan más adelante.

Además, Delt@ dispone de diferentes elementos de control de acceso tanto en el nivel de la información, mediante la generación de un log en el que quedan registrados todas y cada una de las operaciones realizadas por los usuarios registrados y no registrados, como en el de los propios elementos que forman parte del sistema, mediante la activación de las diferentes auditorías, que proporcionan tanto el sistema operativo como la propia base de datos.

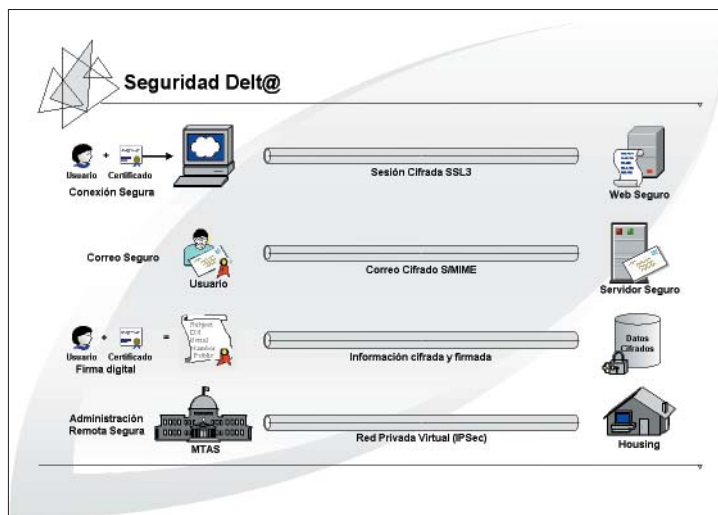
### Conexión segura

Para el intercambio de información se establece una conexión segura SSL. Es en esta conexión segura entre cliente y servidor donde se realiza la identificación mutua entre servidor y cliente a través del intercambio de sus certificados. De este modo ambas partes tienen certeza de con quién están entablando conversación. Además, este tipo de conexión garantiza la confidencialidad, es decir, nadie que no esté autorizado podrá acceder a los datos de la comunicación.

Establecida la comunicación segura, y una vez identificado el usuario en el sistema, es decir, el usuario está registrado y ha sido autenticado por el servidor de políticas, será necesario que toda aquella información de carácter personal que esté sujeta a un nivel de protección alto y se almacene en el sistema sea cifrada conforme a la legislación vigente.

### Cifrado de datos

Delt@ basa el cifrado de datos en procedimientos para el descifrado y el cifrado que utilizan una clave de 192 bits y el algoritmo de clave simétrica Triple DES. El sistema contempla un módulo de gestión de la clave, de manera que en el caso de que la privacidad de la misma pueda haber sido vulnerada, o como medida de seguridad, se pueda proceder a un cambio de clave y por tanto, proceder a un «recifrado» de toda la información contenida en la base de datos.



El sistema Delt@ no sólo contempla el cifrado de datos en el intercambio de información entre cliente y servidor, sino que en las comunicaciones por correo electrónico que implican el envío de datos sensibles también se garantiza la confidencialidad, integridad de los datos y no repudio mediante un procedimiento de firma y cifrado utilizando el protocolo S/MIME.

### Firma digital

Un tema particularmente crítico en Delt@ es el procedimiento de firma y gestión de documentos originales, así como su almacenamiento por un largo periodo de tiempo. Para ello se ha diseñado un sistema de firma y mantenimiento de originales basado en mecanismos de firma digital.

La firma digital es un mecanismo de seguridad que proporciona autenticación (identificación) del firmante, integridad de los datos firmados (asegura si los datos firmados en algún momento han sido modificados) y no repudio (es decir, una vez que se firmaron los datos, no es posible negar posteriormente la autoría). Así, en Delt@ podrá verificarse que los datos enviados en formularios o ficheros firmados proceden del usuario que los ha firmado y no han sido modificados durante su transmisión.

El proceso de firma definido se caracteriza por:

- El usuario realiza la firma con la clave privada de su certificado (que estará en un repositorio del navegador o en una tarjeta inteligente).
- El proceso de firma no sólo implica la firma por parte del usuario, sino que además el servidor realiza una verificación de la firma del usuario y firma con el propio certificado del servidor el resultado de dicha verificación.

- Para la verificación de la firma es necesario disponer del certificado del usuario que la originó. Para ello, Delt@ incorpora en la propia firma los atributos necesarios del certificado para realizar la verificación.

El formato de la firma se ajusta al estándar PKCS#7 del tipo sólo firma, es decir, el paquete de firma generado sólo contiene la firma de los datos, de modo que para el envío de datos y su correspondiente firma, son necesarios dos ficheros. Esta implementación permite evitar posibles problemas en la extracción de los originales desde la firma y agiliza la

obtención de los mismos al almacenarse datos y firma por separado.

Por otra parte, teniendo en cuenta los avances en los sistemas criptográficos, así como los posibles fallos que se puedan detectar en cualquiera de los algoritmos usados en el sistema, es importante tener un sistema de auditoría del estado de los datos firmados. Para ello Delt@ incorpora un procedimiento de refirmado de los originales almacenados por el que un usuario administrador del sistema confirma la integridad y autenticidad de los datos guardados. ■

**MANUEL VILLAVARDE LÓPEZ**  
Responsable Técnico del Proyecto Delt@  
Grupo SIA  
mvillaverde@sia.es