tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

DELT@
Sistema de Declaración Electrónica de Trabajadores Accidentados

Joseba M. García Celada

Jefe de Área de Proyectos Especiales en la Subdirección General de Proceso de Datos del Ministerio de Trabajo y Asuntos Sociales

Miguel A. Gendive Rivas

Jefe de Servicio de Sistemas Informáticos en el Área de Proyectos Especiales de la Subdirección General de Proceso de Datos del Ministerio de Trabajo y Asuntos Sociales.

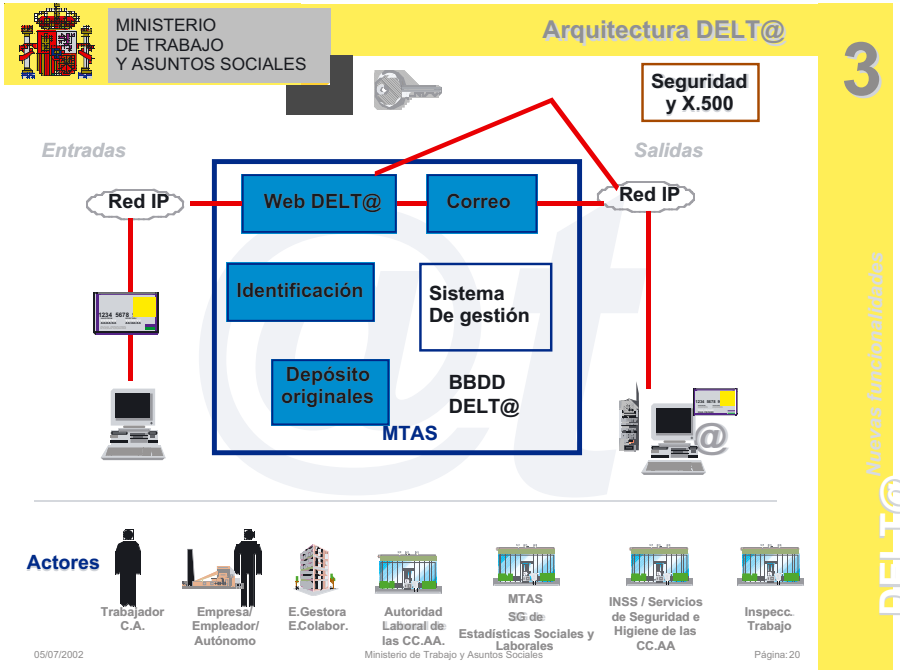
El Sistema Delt@

El Sistema de Declaración Electrónica de Trabajadores Accidentados, tiene como finalidad dar soporte a la tramitación de los Partes de Accidente de Trabajo y otros documentos relacionados con los mismos (Relaciones de Accidentes de Trabajo sin Baja Médica y Relaciones de Altas y Fallecimientos), así como establecer un soporte telemático para la presentación de las Comunicaciones Urgentes de Accidente de Trabajo.

Se trata por tanto de adaptar la Orden de 16 de diciembre de 1987, reguladora del procedimiento de cumplimentación y tramitación de las notificaciones de los accidentes de trabajo, a lo establecido por el Real Decreto 263/1996 de 16 de febrero, por el que, en desarrollo de las previsiones contenidas en la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se regula la utilización de técnicas electrónicas, informáticas y telemáticas por las Administraciones Públicas en sus relaciones con los ciudadanos.

Se pretende dotar a los agentes participantes de una herramienta ágil y segura que permita una más fácil tramitación de los documentos, minimice los errores en su cumplimentación y colabore a la prevención de los accidentes laborales mediante un acceso a los datos con la mayor proximidad posible al momento en que se produzcan los hechos a los que se refieren.

¿Quiénes participan?



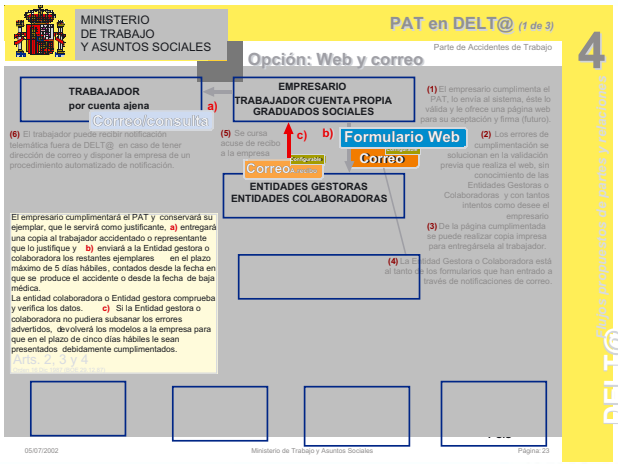
Las empresas y trabajadores por cuenta propia, por sí mismos o a través de sus representantes originan el inicial Parte de Trabajo que remiten a la/s entidad/es gestora/s y colaboradora/s correspondiente/s.

Las Entidades Gestoras y Colaboradoras verifican y, en su caso, completan el parte, remitiéndolo a la Autoridad Laboral competente en cada caso o lo devuelven a la empresa para subsanación de errores.

Reciben también la información de los accidentes el Ministerio de Trabajo y Asuntos Sociales, con fines estadísticos, y, cuando así se prevé en la norma, en función de determinadas circunstancias (gravedad del accidente, entidad aseguradora, etc.), también la Inspección Provincial de Trabajo y Seguridad Social y el Instituto Nacional de la Seguridad Social.

Detalles de algunos aspectos de Delt@

El sistema Delt@ se ha ideado para ser accesible a través de Internet, manteniendo las necesarias garantías de seguridad, al apoyarse sobre la tecnología de certificados de clave pública, tratarse de un sistema de alta disponibilidad y, al propio tiempo, facilitar lo más posible el trabajo de los agentes.



Especialmente singular es que se trata de gestionar el flujo de una tramitación que pasa por diversas etapas en las que participan entes particulares y las administraciones públicas General del Estado y Autonómicas.

Estas características ha llevado a que se diseñe un sistema de registro para el acceso al sistema al menos tan ágil como el utilizado en la previa tramitación de los documentos sobre soporte papel. Si bien las entidades centrales de la tramitación, entidades gestoras y colaboradoras y autoridades laborales, por ser unas las realizadoras de las prestaciones que de los accidentes de trabajo pudieran derivarse y las otras las competentes en la materia, han de registrarse ante el administrador del sistema; los representantes de las empresas, si bien han de estar debidamente autenticados mediante su certificación X.509 expedido con una Autoridad de Certificación reconocida por Delt@, no precisan de más trámite que rellenar su formulario de registro para empezar a operar introduciendo documentos en el sistema.

Inicialmente los datos de las empresas o de los trabajadores por cuenta propia se introducen en el sistema por el usuario de Delt@, si bien se previó la incorporación de la información ya existente en las bases de la Seguridad Social, asociada a cada cuenta de cotización y que, en aplicación de la Ley 30/1992, era deseable no volver a solicitar al administrado, agilizando así de forma notable el proceso de cumplimentación de los documentos.

El gran volumen de documentos que anualmente se tramitan, estimado en un millón de partes de accidentes de trabajo a los que han de añadirse los otros documentos asociados y cuya tramitación por el sistema se ha previsto, hace que se haya tenido en cuenta que los agentes pueden contar con sus propios sistemas informáticos para la cumplimentación de la parte que les corresponde en los documentos y se ha establecido una opción de carga y descarga masiva mediante ficheros de remesas, basada en formatos XML y ASCII.

La alta disponibilidad trata de garantizar el funcionamiento del sistema de forma continuada (aproximarse lo más posible al ideal de 24 horas x 365 días) por lo que ha de contemplarse diversos aspectos:

1. Monitorización continuada de los sistemas.

2. Infraestructura de ubicación que:

a. garantice permanentemente un entorno ambiental adecuado,

b. asegure la no interrupción de la alimentación eléctrica

c. disponga de un control de seguridad para el acceso a las instalaciones

Los puntos 1 y 2 han llevado a contratar un alojamiento externo del sistema (housing), ante la falta de infraestructuras adecuadas del propio departamento.

3. Sistemas con tolerancia a fallos:

a. doble dominio eléctrico, para dos acometidas diferenciadas,

b. sistemas de ventilación redundantes,

c. accesos de red internos y externos (fast ethernet y giga bit) también redundantes,

d. discos configurados en espejo (RAID 1 + 0),

e. servidores de acceso y de aplicaciones con balanceo de carga.

4. Soporte para un elevado número de conexiones simultáneas, no sólo de acceso web sino concurrentes con transferencias de ficheros.

5. Así mismo se han tenido en cuenta las importantes necesidades transaccionales, especialmente notables en los procesos de recifrado de originales almacenados que, periódicamente habrán de acometerse.

Los aspectos relacionados con la seguridad se tratan en un apartado específico.

La Fase Piloto del Proyecto

Durante la segunda quincena de mayo y los meses de junio y julio, se llevó a cabo una prueba piloto del sistema en la que participaron tres entidades gestoras y colaboradoras, que, además de su rol como tales, actuaron como representantes de empresas ficticias, las Autoridades Laborales de dos Comunidades Autónomas y los agentes pertenecientes al Ministerio de Trabajo y Asuntos Sociales.

Esta experiencia resultó de una importancia clave, pues permitió unas últimas adecuaciones de la aplicación a las necesidades detectadas, evaluar el comportamiento del sistema con flujos reales, realizados a través de Internet para poder ver la velocidad de respuesta del sistema en su conjunto y la reacción ante las incidencias propias de las comunicaciones sobre ese medio.

Un aspecto importante fue la adecuación de las ayudas on line y de los manuales a las necesidades de usuarios de muy diferente perfil, especialmente importante, como veremos en el apartado de seguridad, en los momentos de los accesos iniciales de los usuarios al sistema.

Los cuestionarios remitidos por los usuarios proporcionaron una respuesta positiva hacia Delt@ y supusieron un impulso adicional hacia la puesta en marcha definitiva.

Seguridad

En el proyecto Delt@ la seguridad ha sido un aspecto primordial desde el instante del diseño. Esto es así por dos razones evidentes:

1. Se transmiten sobre canales públicos datos personales, algunos incluso de especial sensibilidad, como dictámenes médicos, información sobre lesiones, etc., a los que, según Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, corresponde el más alto nivel de protección.

2. Se trata de sustituir los hasta entonces utilizados documentos sobre papel, con sus firmas y sellos, por originales electrónicos con al menos las mismas garantías, a fin de que den lugar a las mismas consecuencias jurídicas que, en el caso de los accidentes de trabajo se traducen también en efectos económicos y en un soporte esencial en la investigación de los accidentes laborales.

Se establecieron por tanto los siguientes servicios de seguridad:

A) Autenticación de los interlocutores en las conexiones con el sistema, la sesión ha sido iniciada por quién dice ser.

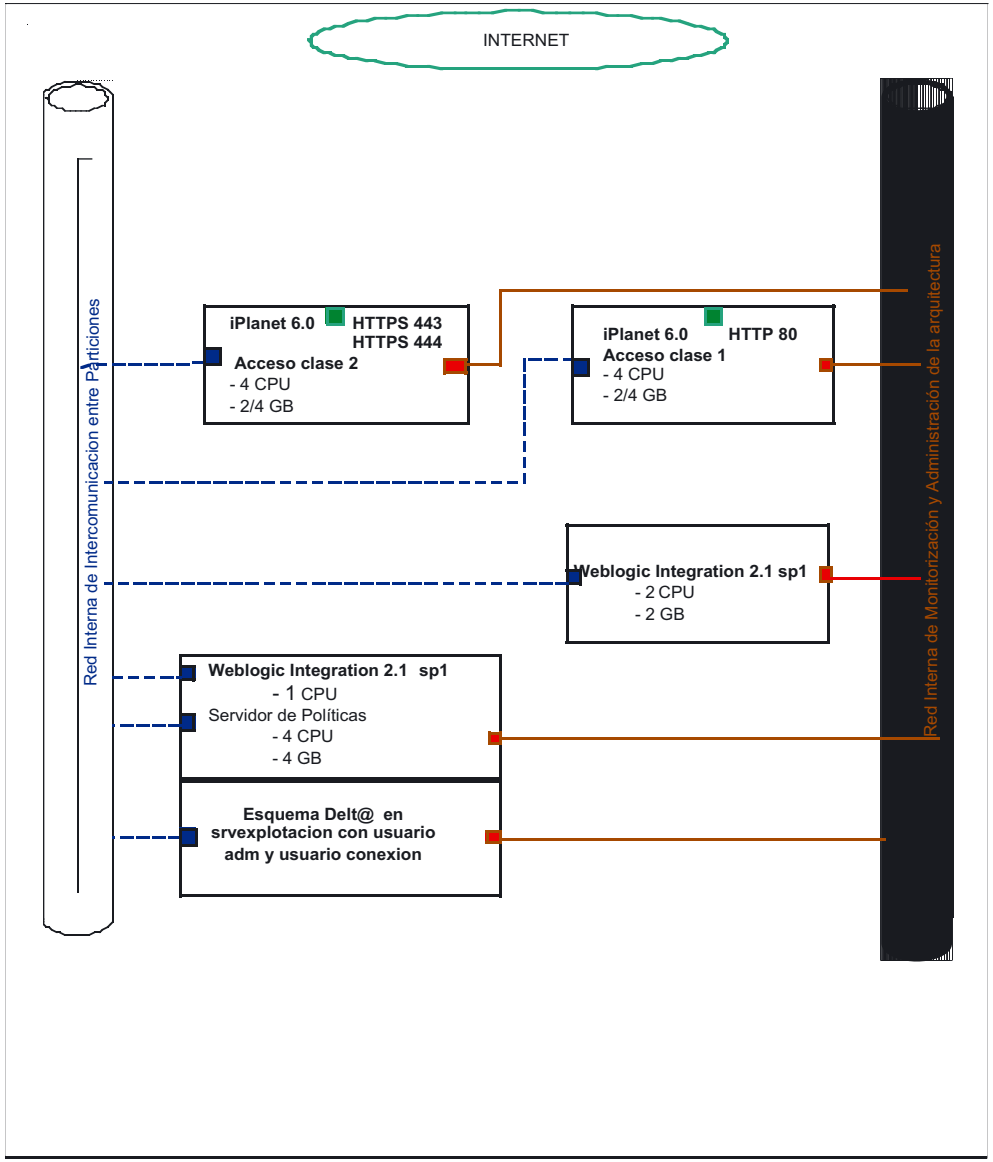
B) Confidencialidad de las comunicaciones mediante cifrado del canal o del mensaje, según se tratase de una sesión web o del envío de un correo electrónico, de forma que sólo los comunicantes pueden acceder a la información transmitida.

C) Autenticación de los autores de cada trámite de un documento, garantizando que se conoce quién ha realizado esa acción.

D) Integridad del documento, no pudiendo haberse producido ninguna alteración sobre el original firmado por el autor.

E) No repudio del envío, por lo que la información almacenada impide que el remitente pueda negar posteriormente haber realizado la acción en el momento que ha registrado el sistema.

Hemos de mencionar también la seguridad de las comunicaciones entre los servidores del sistema, para la que se ha previsto una red privada para las comunicaciones de la aplicación (servidor de seguridad de control de accesos, servidores de aplicaciones y base de datos), siendo el único acceso externo el acceso web con autenticación. Otra red privada dará acceso a los administradores del sistema, soportará la monitorización de alarmas y permitirá la realización de backups y restauraciones de datos.


INTERNET
Red Interna de Intercomunicacion entre Particiones
iPlanet 6.0 HTTPS 443
HTTPS 444
Acceso clase 2
- 4 CPU
- 2/4 GB
iPlanet 6.0 HTTP 80
Acceso clase 1
- 4 CPU
- 2/4 GB
Weblogic Integration 2.1 sp1
- 2 CPU
- 2 GB
Weblogic Integration 2.1 sp1
- 1 CPU
Servidor de Políticas
- 4 CPU
- 4 GB
Esquema Delt@ en srvexplotacion con usuario adm y usuario conexion
Red Interna de Monitorización y Administración de la arquitectura

Uso de Certificados para autenticación y firma electrónica

La política de seguridad de Delt@, como se ha indicado, prevé el acceso a través de certificados de clave pública X.509, inicialmente de los emitidos por la FNMT, del tipo 2 CA. Estos certificados cumplen el estándar X.509 v3 y están dotados de un algoritmo de firma sha1 RSA con una clave de 1024 bits. La pareja de claves contenida en cada uno de ellos, está prevista para su uso tanto para firma electrónica como para cifrado.

La política de seguridad de Delt@ prevé reconocer otras posibles Autoridades de Certificación, a petición de los agentes participantes. En este sentido se hace una clara expresión de voluntad de incorporar el uso de firma electrónica reconocida, que cumpla los requisitos previsto en el artículo 5.1 de la Directiva de la Unión Europea 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 y en el artículo 3.1 del Real Decreto-Ley 14/1999 de 17 de septiembre, cuando ésta esté disponible[1], a fin de garantizar que las firmas de documentos del sistema disfruten en todo caso de la presunción de equivalencia con la firma manuscrita.

Al no disponer de, ni estar previsto, por ahora, un sistema de confianza entre autoridades de certificación, ni tampoco algo similar al federal norteamericano, de una autoridad puente entre autoridades de certificación (bridge CA), ni tampoco certificaciones cruzadas entre nuestro proveedor de servicios de certificación, la FNMT, y el resto de Autoridades de Certificación existentes, esa confianza ha de establecerse localmente en el servidor, agregando los certificados raíz de aquellas Autoridades de Certificación que Delta considere de confianza y realizando la consulta del estado de revocación de cada certificado a través del sistema previsto en el certificado.

La comunicación entre el usuario y el servidor de acceso de Delt@ se establece mediante un canal SSL, con autenticación basada en los certificados de servidor y cliente y cifrando la información con una clave de 128 bits. Por tanto, cuando el usuario intenta acceder al sistema, debe identificarse con un certificado válido y reconocido por el sistema.

1 *Para ello habrán de entrar en servicio los registros previstos en el Real Decreto-Ley y sus normas de desarrollo, en los ministerios de Justicia y Fomento, para los prestadores de servicios de certificación y para aquéllos que decidan acreditarse voluntariamente; se aprueben los estándares por el Comité previsto en el artículo 9 de la Directiva y se publiquen en el DOCE y en el BOE, se produzca la certificación de las entidades y dispositivos conformes con esos estándares...*

Una excepción es el caso de la presentación de comunicaciones urgentes de accidentes graves, pues en aplicación de lo previsto la Orden de 16 de diciembre de 1987 que admitía la más amplia gama de vías para su comunicación siempre que fuese escrita, se permite la presentación por usuarios no registrados y que carezcan de certificado, que, en todo caso, han de rellenar un formulario de registro con datos identificativos básicos. En este caso se establece una comunicación SSL, en la que sólo el servidor está autenticado, pero en la que la confidencialidad de la información transmitida está igualmente garantizada por el cifrado de 128 bits. El sistema advierte a los receptores de las comunicaciones urgentes que hayan sido presentadas por usuarios no identificados mediante un certificado de que, debido a esa circunstancia, no puede garantizar la autenticación del remitente.

La puesta en marcha del sistema anterior no ha sido tan sencilla como pudiera parecer inicialmente, pues en la fase piloto, aparecieron problemas imprevistos: ante la falta de estándares antes indicada, en los certificados que emiten las diversas autoridades de certificación, se producen diferencias en el número de campos incluidos en el certificado y el contenido de los mismos, en los formatos, aún respetando las especificaciones X.509, como los juegos de caracteres empleados y la interacción del software de lectura de las tarjetas con el navegador y el software de verificación del servidor.

Otro aspecto relevante se deriva de que el acceso se produce en muchas ocasiones desde puestos conectados a una red de área local, de una gran empresa o de una administración pública, con sus sistemas de seguridad periférica, sus políticas de configuración, perfiles de usuario, niveles de actualización de la versión de los navegadores no fáciles de mantener, etc. a estas circunstancias ha de agregarse que el soporte informático al usuario no siempre es un interlocutor próximo del mismo por lo que solventar las técnicamente sencillas incidencias (puertos a utilizar y que por tanto han de estar autorizados en los firewall, derechos de escritura y descarga para la instalación de los certificados, configuración de proxy, etc.) no resultan siempre fáciles de diagnosticar y de solventar.

Gestión de originales

Los originales almacenados han de permanecer en el sistema durante un largo plazo, ya que puede ser necesario acceder a ellos varios años después de que se produjese un accidente de trabajo. Técnicamente nos lleva al problema de

que las claves con las que los documentos fueron firmados o los algoritmos utilizados pueden dejar de ser considerados fiables (por ejemplo la revocación o caducidad de un certificado).

Para afrontar este problema los documentos introducidos en el sistema y los datos de verificación de firma son refirmados por el administrador y se ha previsto que, periódicamente o ante incidencias que pudiesen afectar a las claves del administrador, se proceda a refirmar los originales. El proceso puede repetirse tantas veces como se precise, para recuperar el original, se comprobarán primero la firma de refirmado y los datos de verificación de la firma original.

La seguridad va más allá, como hemos indicado, hay datos que requieren de un nivel de protección alto y que, por tanto, han de ser cifrados para su almacenamiento.

El sistema ha de contemplar no sólo campos sensibles de forma individualizada, sino que ha de tenerse en cuenta que se almacenan documentos originales, generados por el usuario como un todo, pues es el documento que ha firmado y el que del sistema deberá recuperarse para su presentación como prueba incluso judicial[2].

Una vez más, el largo periodo de almacenamiento, lleva a que el sistema de cifrado de la base de datos, tenga que prever la posibilidad de un recifrado periódico con un nuevo algoritmo o con una clave más larga cuando, de acuerdo con los criterios de seguridad establecidos, se considere necesario.

2 En Delt@ el original no es necesariamente un Parte de Accidente de Trabajo o una Relación de Altas y Fallecimientos individualizado, pues puede tratarse de una remesa que, en un solo original firmado, incluya incluso cientos o miles de documentos.

Registro de accesos

Lógicamente Delt@ guarda registros de todos los accesos realizados al sistema, con indicación del usuario, fecha y hora, operación realizada, etc. que permite obtener una traza de todas la operaciones.

Correo seguro S/MIME

Los actores del sistema y otros destinatarios, como las Inspecciones Provinciales de Trabajo y Seguridad Social y el Instituto Nacional de la Seguridad Social, reciben mensajes de correo electrónico que han de estar protegidos frente a posibles alteraciones y, cuando llevan datos personales, también frente a accesos no autorizados, es decir se requiere también aquí autenticación, integridad, confidencialidad y no repudio del envío. Para este fin Delt@ utiliza S/MIME, apoyándose en los certificados X.509, lo que requirió una actualización de la infraestructura de correo electrónico del MTAS.

En este punto cobra singular importancia la dirección de correo electrónico que aparece en el certificado, pues al ser este un certificado personal del usuario éste puede haber facilitado una dirección particular ni siquiera accesible desde su puesto de trabajo, con limitaciones en el tamaño de su buzón y/o que cambie durante la vigencia del certificado. Más críticos aún resultan posibles errores en la dirección de correo electrónico que figura en el certificado, pues impide de la remisión de los mensajes por el sistema y, para solventarlo, el usuario ha de acudir a revocar su certificado y solicitar uno nuevo.