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
www.tecnimap.com
Ponencias

Política de certificación en la Seguridad Social

Carlos Escudero Rivas

Director del Centro de Seguridad de la Subdirección General de Informática de la Tesorería General de la Seguridad Social

La Seguridad Social en su interés por proporcionar al ciudadano acceso a servicios de formas más ágiles y cómodas, ofrece la posibilidad de la realización de diversos trámites y operaciones a través de medios telemáticos. Estos trámites, al ser realizados utilizando redes públicas, entre otras Internet, deben ser dotados de las medidas de seguridad que proporcionen las garantías al ciudadano.

Las políticas de seguridad son el conjunto de normas que guían y respaldan las medidas de seguridad (tanto desde el punto de vista técnico como de gestión). Las políticas de seguridad se dictan con el fin de proteger los activos de una organización. Los contenidos o activos de negocio son los valores corporativos que deben ser protegidos. Difieren mucho de una organización a otra ya que pueden ser tangibles (sistemas informáticos, redes, personas, documentos, etc.) o intangibles (imagen, reputación de empresa, legales, confianza, servicios, etc.).

¿Qué activos ofrece la Seguridad Social en Internet?

La Seguridad Social ofrece en Internet diversos tipos de información:

a) Información de carácter público: normativa, tablas de valores, ubicación de oficinas, cartas de servicios, etc. Esta información está protegida mediante los mecanismos físicos y lógicos establecidas por las políticas de seguridad de la Seguridad Social.

b) Información de carácter confidencial proporcionada a través de servicios:

- Servicios orientados al ciudadano que permiten la consulta de datos de carácter personal.
- Servicios de actualización y consulta sobre todo enfocados a representantes de empresas y que permiten realizar gestiones con la Seguridad Social.

La información confidencial requiere unos servicios básicos de seguridad:

Confidencialidad, integridad, autenticación, no repudio, control de acceso y disponibilidad.

El mecanismo utilizado en Internet para proporcionar los servicios básicos de seguridad es la certificación de clave pública.

Infraestructura de clave pública (PKI).

Una infraestructura de clave pública (PKI) es el conjunto de hardware, software, personal, políticas y procedimientos para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública.

Los elementos que integran esta infraestructura son los siguientes:

- Entidades a certificar:
    i. certificados personales
    ii. certificados de servidores
    iii. certificados para firma de objetos y código
    iv. certificados para entidades
- Autoridades de Certificación (CA)
- Autoridades de Registro (RA)
- Repositorio de certificados.

Definiciones

Certificado: Documento emitido y firmado digitalmente por una Autoridad de Certificación (CA) que asocia el nombre distintivo de una entidad con su clave pública durante un periodo de tiempo.

Autoridad de Certificación (CA): Entidad encargada de gestionar la emisión / generación de certificados y revocaciones.

Autoridad de Registro (RA): Entidad encargada de4 recoger las solicitudes de certificación y revocación, Comprueba y autentica la identidad de los solicitantes y entrega las solicitudes validadas a la CA.

Repositorio de certificados: Es una base de datos de certificados disponibles. Suele utilizarse servidores de directorio basados en X.500 y LDAP.

Políticas de certificación de una PKI.

El primer nivel en la política de certificación viene proporcionado por la infraestructura de PKI.

Según el estándar X.509 la política de certificación es: " un conjunto de reglas que indican la aplicación de un certificado para una comunidad en particular y / o un tipo de aplicación con requisitos de seguridad comunes".

El árbol de políticas de certificación de una PKI afecta por un lado a la encriptación (confidencialidad) y por otro a asegurar distintos niveles de firma digital.

En general, las políticas implementadas por las PKI aseguran que un certificado pueda permitir distintos niveles de firma electrónica o de cifrado, pero no de ambos.

El caso español: proyecto CERES.

El sistema de certificación de la Administración española se ha puesto en práctica mediante el proyecto CERES, en el que se ha constituido la Fábreica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM) como Autoridad de Certificación. Como tal autoridad de Certificación necesita haber realizado una Declaración de Prácticas de Certificación, donde se indica el ámbito de certificación, los posibles usos de los certificados, las responsabilidades que

asume y las que deben asumir los titulares de certificados, así como las medidas técnicas y de seguridad empleadas para la generación de certificados digitales.

El sistema tecnológico y de seguridad elegido por la FNMT-RCM se encuentra dentro de los denominados de Infraestructura de clave pública (PKI).

Todos los elementos tecnológicos, salvo las oficinas de registro, residen en la REAL FÁBRICA DE MONEDA Y TIMBRE y utilizan software PKI para ejercer los servicios de Certificación.

CLASES DE CERTIFICADOS EMITIDOS POR LA FNMT- RCM

En función de los niveles de garantía, la FNMT-RCM tiene definidas las siguientes clases de certificados, enumeradas de mayor a menor nivel de seguridad:

- FNMT Clase 1 CA
- FNMT Clase 1S CA
- FNMT Clase 2 CA

Tabla comparativa de clases (fuente FNMT-RCM):

Clase	Tipo de Registro	Emisión del Certificado				Gestión y uso	
		Generación de claves	Uso de las claves	Longitud mínima	Soporte Físico	Software de gestión de Certificados	Hardware Tarjeta
FNMT Clase 1 CA	Presencial	Por la FNMT	2 pares independientes para firma y cifrado	1024 bits	Tarjeta Criptográfica	Proporcionado por la FNMT	Proporcionado por la FNMT
FNMT Clase 1S CA	Presencial	Por la FNMT	2 pares independientes para firma y cifrado	1024 bits	Software	Proporcionado por la FNMT	No aplicable
FNMT Clase 2 CA	Presencial	Por el usuario	1 par para ambos usos	Sin límite	Software ó Tarjeta Criptográfica	Comercial	En caso de utilizar Tarjeta Criptográfica, esta es proporcionada por la FNMT

Características técnicas de los certificados

A continuación se enumeran las características técnicas y funcionales de los anteriores certificados (FNMT Clase 1 CA, FNMT Clase 1S CA, FNMT Clase 2 CA) que pueden ser emitidos a ciudadanos para realizar tareas administrativas.

FNMT Clase 1 CA.

Este certificado se encuentra en el interior de una tarjeta inteligente y las operaciones de firma se realizan en el interior de la misma. Es el nivel más alto de seguridad y el que, actualmente, emplean los registradores de certificados en las Unidades de Atención al Usuario, en el caso de la Tesorería General de la Seguridad Social.

FNMT Clase 1S CA.

Este certificado requiere de un software instalado en los puestos cliente que se encarga de realizar todas las operaciones criptográficas necesarias, además de controlar que los certificados utilizados no estén revocados o suspendidos. Esta gestión de los certificados, además de la gestión del canal de comunicación es realizada de forma propietaria por dicho software.

Para dotar de mayor nivel de seguridad a su utilización, este tipo de certificados requiere para su emisión que el usuario se persone físicamente en las oficinas de registro autorizadas para ello. De esta forma se evita que existan situaciones irregulares en la identificación del usuario.

FNMT Clase 2 CA.

Este certificado, a diferencia del FNMT Clase 1S CA, no requiere de software específico de cifrado en el puesto cliente, ya que el navegador (en el caso web) o la herramienta de correo electrónico disponen de UN mecanismo cripto-

gráfico de funcionalidad análoga, aunque no tan eficiente ni segura como la infraestructura utilizada en el certificado FNMT Clase 1S CA.

Es necesario, sin embargo, la necesidad de un software para gestionar tanto la firma electrónica como el cifrado de la información enviada a través del canal de comunicación pero como se apoya en gran medida en las funciones del navegador esto implica que dicho software sea ligero para transmitir por Internet en cada conexión.

Este certificado aunque puede ser grabado en un disquete, deja información del mismo, por lo tanto del usuario, en el equipo donde esté instalado.

Para dotar de mayor nivel de seguridad a su utilización, este tipo de certificados requiere para su emisión que el usuario se persone físicamente en las oficinas de registro autorizadas para ello. De esta forma se evita que existan situaciones irregulares en la identificación del usuario.

El certificado FNMT Clase 2 CA anterior puede ser introducido en el interior de una tarjeta inteligente, dotándolo de un nivel superior de seguridad.

El funcionamiento de esta variante del certificado FNMT Clase 2 CA, es ligeramente distinto a la versión software. De hecho, es necesario realizar un desarrollo que permita al navegador o herramienta de correo electrónico que se utilice, el acceso a la tarjeta y a los servicios que ésta proporcione.

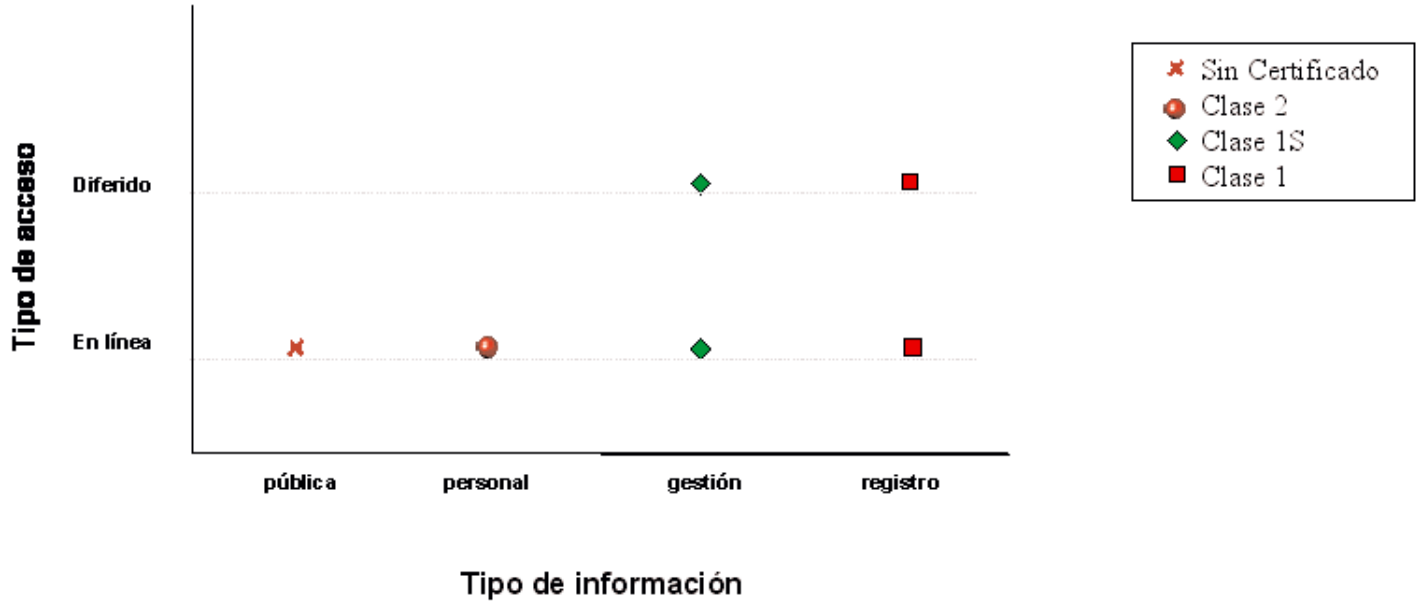
Políticas de certificación de la Seguridad Social.

En la actualidad la Seguridad Social posee una plataforma de seguridad basada en certificados digitales emitidos gestionados a través de procedimientos de software proporcionados por CERES que permite tanto al ciudadano como a las empresas y graduados sociales realizar consultas y operaciones con ella.

La política de certificación de la Seguridad Social es una malla de posibilidades de interconexión entre tipos de acceso (en línea y diferido) y los tipos de información a proteger de forma que para cada tipo de información puede tener una política diferente según sea el tipo de acceso a realizar sobre el dato.

Esto viene inducido por los distintos niveles de protección que proporcionan los distintos certificados de la FNMT. Así, es crítico distinguir entre las funcionalidades de cifrado y de firma electrónica y la conveniencia de no utilizar los certificados de firma para cifra. Otro aspecto relevante en las necesidades de protección de los sistemas de la Seguridad Social es la necesidad de disponer de certificados de servidores que son esenciales para los servicios de gestión del proyecto RED ya que el envío diferido de peticiones requiere de estos así como un sistema de acuses de recibo.

Cuando la información es pública el acceso es en línea y se permite el acceso sin identificación personal. Cuando la información es confidencial de tipo personal y el acceso es en línea generalmente usando formularios y no es necesario la gestión de ficheros se recomienda el uso de certificados FNMT Clase 2 CA. Si el tipo de acceso afecta a usuarios que realizan gestión, tanto en línea como diferida, con la Seguridad Social y en particular usuarios del sistema RED o de Mutuas se deben utilizar certificados FNMT Clase 1 CA. Las oficinas de registro deben utilizar para los registradores el tipo de certificado recomendado por la CA, en el caso de las oficinas de la Seguridad Social se usan certificados FNMT Clase 1.



Dependiendo del tipo de relación entre ciudadano y la organización y de la cobertura legal exigida, el sistema empleado difiere básicamente entre procesos que tienen o no la posibilidad de generar y / o enviar ficheros de datos personales.

Usuarios que realizan actividad de Registro

La Tesorería General de la Seguridad Social se ha constituido en Entidad de Registro y como tal ha habilitado un número considerable de su personal para que realicen este tipo de tareas. Son las personas que verifican la identidad de los ciudadanos y permiten que el proceso de emisión de un certificado pueda seguir su curso.

Este tipo de usuarios utilizan un certificados FNMT Clase 1 CA, emitidos por CERES. Esto permite un alto nivel de seguridad en todas las gestiones que realizan.

Usuarios que realizan gestión con envío de ficheros

En la actualidad los usuarios que realizan este tipo de gestiones son los que pertenecen a los colectivos del sistema RED y Mutuas Patronales. Como consecuencia de su actividad requieren funciones tanto de firma que demuestre su identidad como de cifrado que aseguren la confidencialidad de la información que va a ser transmitida.

Este tipo de usuarios poseen para sus gestiones de un certificado de Clase 1S emitido por CERES del que usan una pareja de claves como autenticación y otra como firma de sus ficheros llamados de remesas, conteniendo información sensible utilizada en su trabajo.

Resto de usuarios

El conjunto de operaciones que realiza consultas y / o gestiones si se realiza de forma en línea y a través de formularios web requiere la función de identificación, y la confidencialidad de la información que puede lograrse cifrando convenientemente el canal de conexión establecido en ese momento, en similitud a los procesos realizados por otras Administraciones, en particular la tributaria.

Servicios ofrecidos a los ciudadanos