

## PRACTICAS 4 - IDENTIDAD DIGITAL – TEMA 2 – SAD

### a) Firma digital de un documento

- En GNU/Linux: gpg.

En la práctica anterior hemos hecho con el agente gpg una clave privada y pública, ahora lo que vamos a hacer es con un documento que tenemos en el escritorio que se llama md5sumlales una firma digital de este documento, para ello ponemos el siguiente comando

Gpg -sb -a md5sumlales

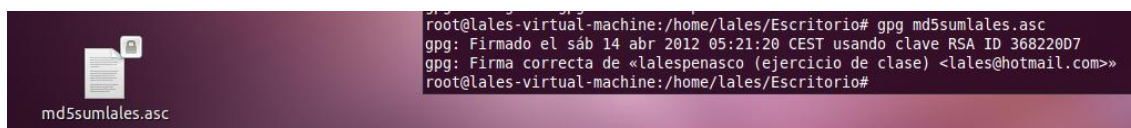
```
root@lales-virtual-machine:/home/lales/Escritorio# gpg -sb -a md5sumlales
Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "lalespenasco (ejercicio de clase) <lales@hotmail.com>"
clave RSA de 2048 bits, ID 368220D7, creada el 2012-04-14

gpg: el agente gpg no esta disponible en esta sesión
root@lales-virtual-machine:/home/lales/Escritorio#
```

A continuación tenemos que poner gpg md5sumlales.asc para que solo pueda ser leído por medio de la contraseña

```
root@lales-virtual-machine:/home/lales/Escritorio# gpg md5sumlales.asc
gpg: Firmado el sáb 14 abr 2012 05:21:20 CEST usando clave RSA ID 368220D7
gpg: Firma correcta de «lalespenasco (ejercicio de clase) <lales@hotmail.com>»
root@lales-virtual-machine:/home/lales/Escritorio#
```

Y nos dice que la firma es correcta y nos aparece el fichero con el símbolo del candado, ya que este documento se ha certificado correctamente



```
root@lales-virtual-machine:/home/lales/Escritorio# gpg md5sumlales.asc
gpg: Firmado el sáb 14 abr 2012 05:21:20 CEST usando clave RSA ID 368220D7
gpg: Firma correcta de «lalespenasco (ejercicio de clase) <lales@hotmail.com>»
root@lales-virtual-machine:/home/lales/Escritorio#
```

md5sumlales.asc

## b) Certificados digitales.

Busca que Autoridades Certificadoras Admitidas de certificados digitales existen en España.

- AC Camerfirma SA
- Agencia Catalana de Certificación
- Agencia Notarial de Certificación S.L. Unipersonal
- ANF Server CA
- Banesto S.A.
- CA Generalitat Valenciana
- Consejo General de la Abogacía
- Dirección General de la Policía
- Firma profesional S.A.
- Fábrica Nacional de Moneda y Timbre
- IZENPE
- Servicio de Certificación de los Registradores

Describe el proceso para la obtención del certificado digital. Visita la web [www.fnmt.es](http://www.fnmt.es)

- 1) **Solicitud vía internet de su Certificado.** Al final de este proceso obtendrá un código que deberá presentar al acreditar su identidad.
- 2) **Acreditación de la identidad en una Oficina de Registro.** Si usted ha solicitado un certificado de persona física, puede dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.
- 3) **Descarga de su Certificado de Usuario.** Unos minutos después de haber acreditado su identidad en una Oficina de Registro, haciendo uso del código de solicitud obtenido en el paso 1, podrá descargar su certificado desde esta página web entrando en el apartado Descarga del Certificado. **NOTA:** Si usted ha elegido una Oficina de Registro de la Agencia Tributaria para acreditar su identidad, debe esperar al día siguiente para proceder a la descarga del certificado.
- 4) **Copia de seguridad. Paso recomendado.**

¿Es válido para todos los navegadores web?

INTERNET EXPLORER Puede optar por una de las siguientes opciones:

- Configurador FNMT-RCM . Para instalar este software es necesario tener permisos de administrador. Al instalarlo se realizan las siguientes tareas: Instala todos los certificados de las CAs raíces e intermedias. Instala la librería Capicom. Realiza modificaciones en el registro de Windows para configurar las opciones de seguridad de su navegador.

FIREFOX Para Firefox es necesario instalar el certificado raíz de la FNMT-RCM, **AVISO: El resto de navegadores no están soportados.**

¿Puede emplearse para firmar otro tipo de archivos?

Si

¿Es posible exportarlo o solamente se puede emplear en un solo equipo?

Técnicamente es posible instalar el certificado digital en más de un equipo a través de las opciones de "Exportar" e "Importar" propias del navegador, pero por motivos de Seguridad se recomienda que este proceso sea realizado única y exclusivamente si es necesario. Es posible exportar la firma electrónica si se trata del certificado de DNI, porque haremos uso del lector. Si se trata del usuario electrónico el certificado está instalado en nuestro navegador, entonces no podemos exportarlo en diferentes equipos.

¿Qué precauciones podemos tener con el certificado digital en cuanto a protección mediante contraseñas a la exportación?

Las precauciones que debemos utilizar es, tener contraseñas con mayúsculas, minúsculas, números, caracteres especiales, la contraseña debe tener un mínimo de 8 dígitos, y se debe cambiar cada cierto tiempo para mayor seguridad.

### **c) Certificados digitales.**

Revisa en la web [www.camerfirma.com](http://www.camerfirma.com), uno de los usos que tiene el certificado digital para la firma y el envío de correos electrónicos con certificado digital.

El uso de un certificado nos garantiza: - La identidad del emisor y del receptor de la información (autenticación de las partes) - Que el mensaje no ha sido manipulado durante el envío (integridad de la transacción) - Que sólo emisor y receptor vean la información (confidencialidad) - Que el receptor de la firma obtenga las evidencias suficientes para probar la relación entre el firmante y los datos firmados (compromiso o no repudio).

**Describe el proceso.**

Su uso es validar documentos de manera electrónica. Para que un certificado digital tenga validez legal, la autoridad de certificación debe de estar acreditada por la entidad pública de certificación del país correspondiente. En España es CERES (Certificación Española) la entidad que se encarga de gestionar este tipo de certificados. El proceso de envío de correos electrónicos con certificado digital sería el siguiente: debemos tener un gestor de correo como por ejemplo thunderbird. Empezamos a redactar el mensaje y cuando este redactado, colocamos la dirección, para validar nuestro correo con el certificado digital pulsamos en seguridad, cifrar mensaje y enviar, así estará firmado digitalmente. Se trata de una aplicación

ideal para el envío masivo de documentos electrónicos (firmados con un certificado digital) a clientes, proveedores y empleados, como pueden ser facturas, pedidos, notificaciones o nóminas, con toda seguridad técnica y legal que aporta la firma electrónica.

### ¿Qué garantiza?

- Que todos los documentos firmados tendrán plena validez jurídica.
- Tendrán alcance internacional.
- Serán adaptables a cualquier necesidad de firma electrónica de documentos.
- Ahorro de costes en el envío.
- Imagen innovadora y avanzada.
- Reducción en los tiempos de tramitación.
- Mejora en los canales de comunicación con clientes y proveedores.
- Facilidades al receptor.

### ¿Qué es S-MIME?

**El S/MIME** (Secure MIME o Secure Multipurpose Mail Extension) es un proceso de seguridad utilizado para el intercambio de correo electrónico que hace posible garantizar la confidencialidad y el reconocimiento de autoría de los mensajes electrónicos. El S-MIME está basado en el estándar MIME, cuyo objetivo es permitir a los usuarios adjuntar a sus mensajes electrónicos archivos diferentes a los archivos de texto ASCII (American National Standard Code for Information Interchange). Por lo tanto, el estándar MIME hace posible que podamos adjuntar todo tipo de archivos a nuestros correos electrónicos.

## d) Certificados digitales.

Realiza los trámites para la obtención de tu certificado digital.

### ¿Dónde lo tienes que descargar?

Hay que descargarlo en la página oficial [www.fntm.es](http://www.fntm.es)

### ¿Dónde tienes que ir a recogerlo?

En una oficina de este Ministerio

### ¿Qué caducidad posee?

Dos años desde el día de la obtención de éste.

Una persona que acceda a nuestro equipo en el que tenemos instalado un certificado digital, ¿puede acceder a distintos sitios web de información personal de tipo legal?

Si

## e) Certificados digitales/ DNle.

Realiza una búsqueda de los servicios de empresas como bancos, y de la administración pública (seguridad social, hacienda, etc) a los que se puede acceder de forma segura, mediante certificado digital y mediante DNle.

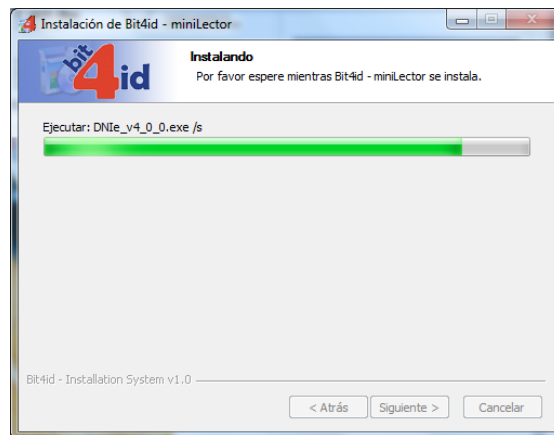
- Acceder a un organismo público en Internet utilizando el Dni-e.

Introducimos el CD de instalación en la disquetera y nos sale un asistente





Le damos a siguiente y vamos instalando

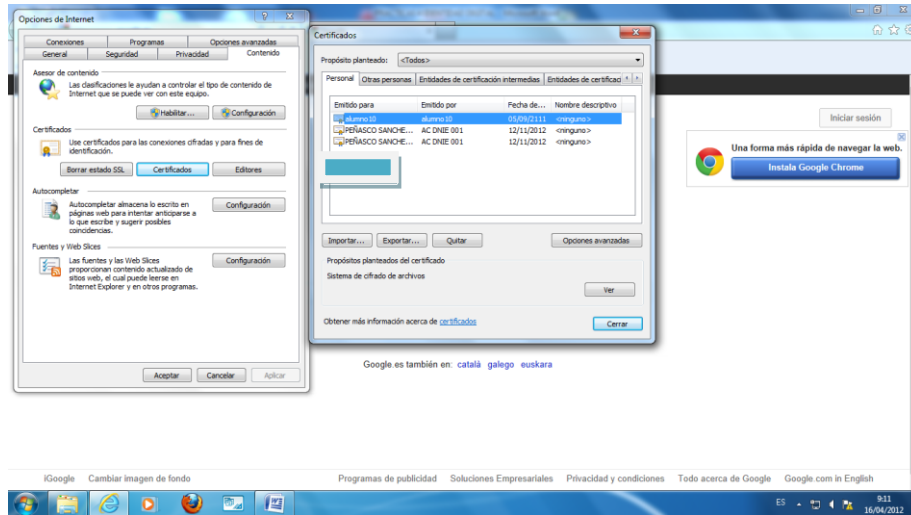


Una vez completado salimos del asistente

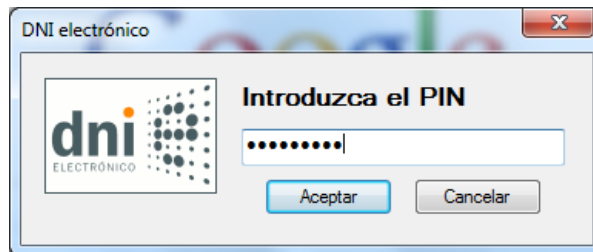


Y ponemos el lector de DNIE en el USB y metemos el dni

Ahora nos vamos a Internet Explorer y en opciones de Internet, le damos a la pestaña de Contenido y luego a Certificados y nos aparece los certificados correspondientes al DNI que tenemos metido en el lector



Nos pide el pin correspondiente



Ahora nos vamos a ir a navegar por una página que nos pida el certificado, vamos a ir a Seguridad Social



## Elegimos sede electrónica y ahí elegimos Servicios con Certificado Digital

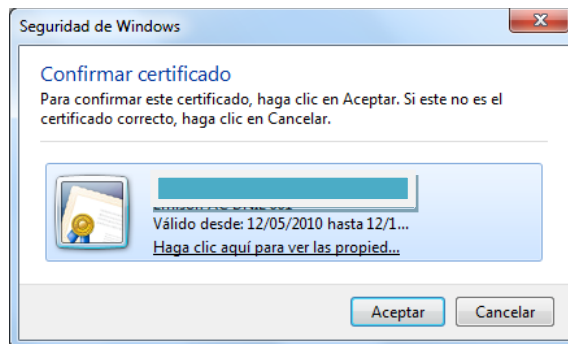
The screenshot shows the 'Seguridad Social sede Electrónica' website. The header includes the Spanish government logo and the text 'GOBIERNO DE ESPAÑA' and 'MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL'. The main navigation bar lists various services like 'Inicio', 'Ciudadanos', 'Empresas y Profesionales', etc. Below the navigation, there are tabs for 'Servicios sin Certificado Digital', 'Servicios con Certificado Digital' (which is selected), and 'Servicios con Certificado SILCON'. The content area lists three services:

- Acreditación actividad agraria cuenta propia.** A través de este servicio se podrá consultar y/o obtener un informe para acreditar la actividad agraria como trabajador por cuenta propia a una fecha determinada o un periodo concreto.
- Asignación de número de la Seguridad Social.** A través de este servicio se puede solicitar la asignación del Número de Seguridad Social, siempre y cuando nunca haya tenido atribuido uno con anterioridad.
- Certificado Provisional Sustitutorio (CPS).** Con este servicio, se facilita la obtención del certificado provisional sustitutorio de la tarjeta sanitaria europea, sólo para el titular del derecho a asistencia sanitaria, en los desplazamientos por Europa.

## Vamos a pedir un informe de base de cotización

The screenshot shows the 'Informe de bases de cotización' page on the 'Seguridad Social sede Electrónica' website. The page title is 'Informe de bases de cotización.' Below the title, there is a link 'Acceso al servicio'. The 'Ámbito' section states: 'Trabajadores incluidos en el Régimen General y asimilados y en los Regímenes Especiales del Sistema de Seguridad Social.' The 'Descripción' section explains that the service allows consulting and obtaining an information report on declared contribution bases for companies or self-employed workers. It also mentions that the report can be obtained through the digital certificate service or the non-certified digital service. A note states: 'En el caso de solicitarlo con certificado digital, la impresión o consulta del informe se realiza en el mismo momento de su petición, a través de su propio ordenador.' At the bottom, there is a 'Requisitos' section with the text: 'Para el servicio con certificado digital:'.

Nos sale un cuadro donde tenemos que decir si esa es la persona que solicita el documento y nos daría la documentación necesaria



**MARÍA ÁNGELES PEÑASCO SÁNCHEZ –ACTIVIDAD 4- TEMA 2 –SAD**