

# Certificado de Origen Digital de ALADI

## Guía de instalación de software

La Firma Digital del Funcionario Habilitado (**FH**) perteneciente a una Entidad Habilitada (**EH**) sólo puede realizarse a través de una Autoridad Certificante (**AC**) legalmente válida en Argentina que posea convenio o sea reconocida por los países miembros de ALADI que estén intercambiando Certificados de Origen Digitales (CODs). Actualmente la única AC registrada en ALADI y reconocida por sus países miembros es la **AC de AFIP** (Administración Federal de Ingresos Públicos).

La AC de la AFIP otorga una Firma Digital a los FH a través de un **dispositivo de hardware** (llave o token) fabricado por la empresa **SafeNET**. Actualmente el dispositivo recomendado es el modelo **iKey 4000**.

Los Exportadores podrán, a criterio de las EHS, utilizar una Firma Digital obtenida en la AC de AFIP o bien en cualquier otra AC legalmente válida en Argentina. Por tanto, las Firmas Digitales de los Exportadores podrán utilizar el token o llave por hardware de SafeNET o cualquier otra que le recomiende la AC que contrate. Incluso también es posible que la Firma Digital contratada no requiere ningún hardware adicional (sólo software).

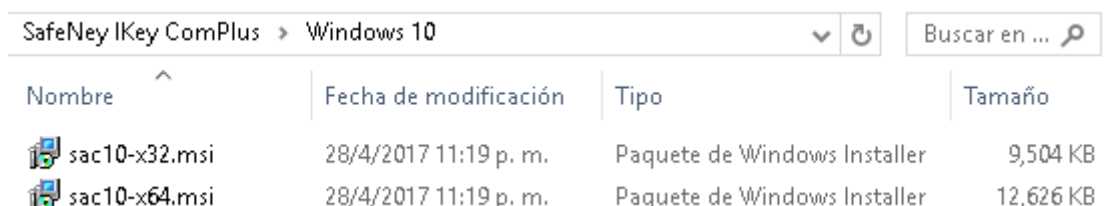
La aplicación informática que permite firmar los archivos XML con el formato COD de ALADI (**DS-COD**) está escrita en lenguaje **JAVA** y son de **distribución gratuita con código fuente bajo la licencia de uso GPLv2**.

Por lo tanto es necesario instalar en el computador del usuario que firmará los Certificados de Origen Digitales (archivos XML con formato COD de ALADI) los “drivers” de la llave o token (hardware) que fueran necesarios y el entorno de desarrollo y ejecución denominados **SDK Java de Oracle** en su versión más actual (1.8).

Los fines de esta **Guía de Instalación** es realizar un paso a paso para instalar el “driver” del token **SafeNET iKey 4000**, el **SDK Java de Oracle**, la aplicación **DS-COD**, el “driver” en **Mozilla Thunderbird**, y la extracción del archivo con el certificado (clave pública) de la AC de la AFIP (**.PEM**).

## Instalación de SafeNET iKey 4000

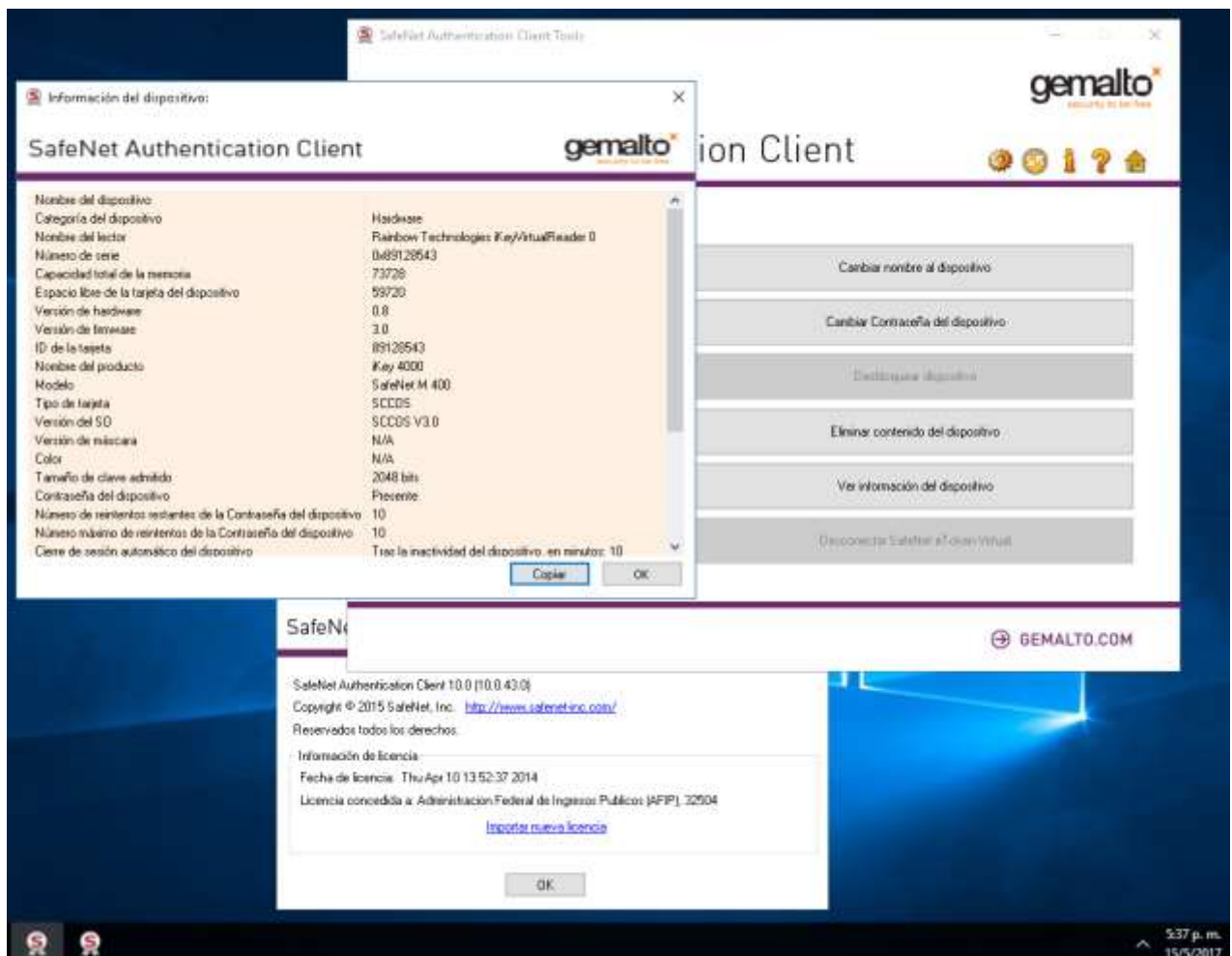
Dependiendo de la plataforma, debe ejecutar el instalador provisto por el fabricante. En el ejemplo, vamos a instalar el software en su versión para Windows 10 en 32 bits.



Nombre	Fecha de modificación	Tipo	Tamaño
sac10-x32.msi	28/4/2017 11:19 p. m.	Paquete de Windows Installer	9,504 KB
sac10-x64.msi	28/4/2017 11:19 p. m.	Paquete de Windows Installer	12,626 KB



Una vez concluida la instalación, introduzca el token en una ranura USB de su computadora, abra desde el área de notificaciones (abajo en la izquierda de su pantalla) el ícono que tiene una “S” roja y acceda a consultar la información del mismo.



Es recomendable abrir la opción “Herramientas” (“Tools” en inglés) y cambiar la contraseña del dispositivo.

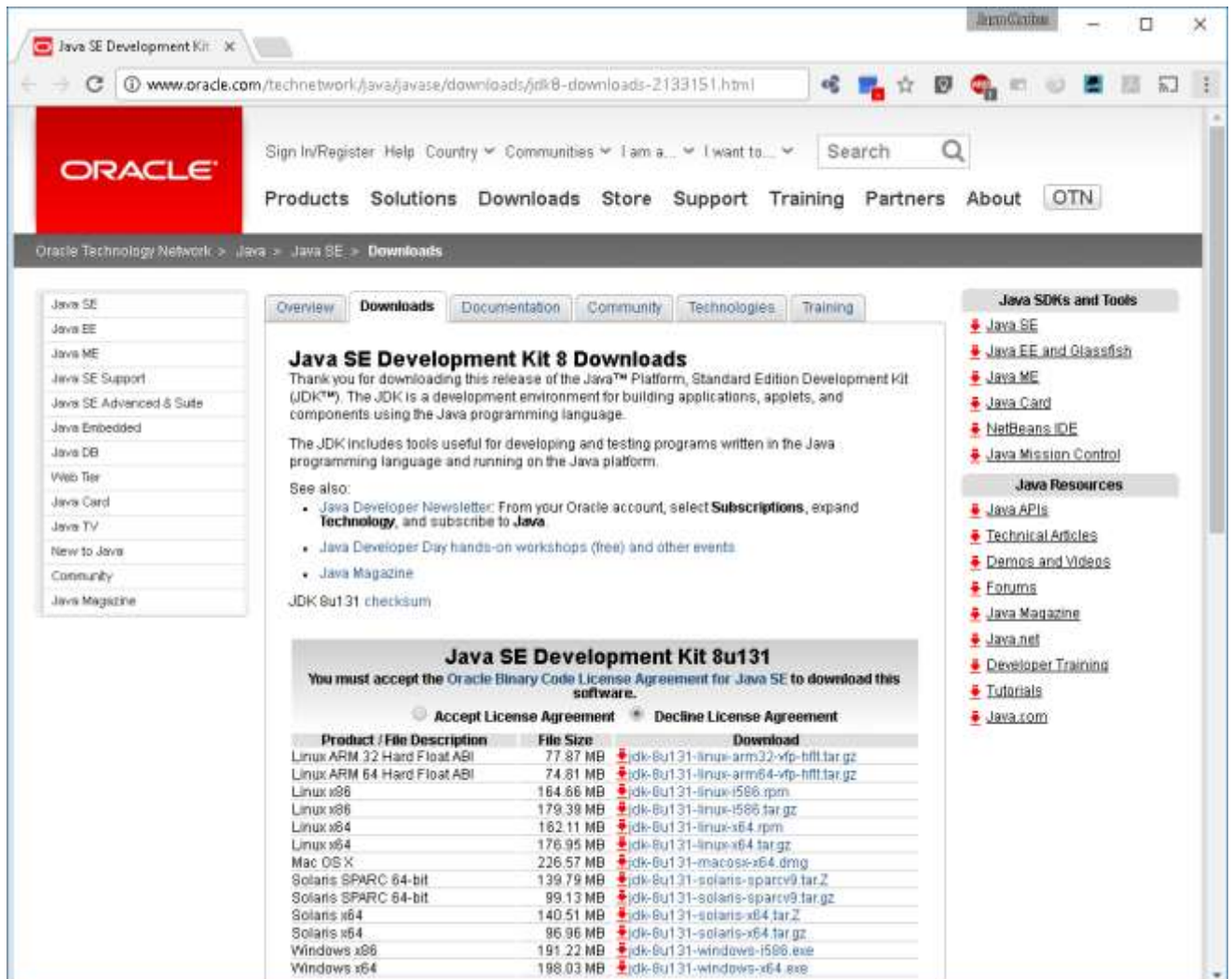
Recuerde muy bien la contraseña que asigne. Fallos reiterados en la contraseña pueden dejar su Firma Digital inválida.

## Instalación de SDK de Java de Oracle

Desde la página web de descargas de Oracle copie a su computadora el instalador del SDK de JAVA que aplique a su plataforma.

La página de descargas de Oracle está en la siguiente ubicación:

<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>



**Java SE Development Kit 8 Downloads**

Thank you for downloading this release of the Java™ Platform, Standard Edition Development Kit (JDK™). The JDK is a development environment for building applications, applets, and components using the Java programming language.

The JDK includes tools useful for developing and testing programs written in the Java programming language and running on the Java platform.

See also:

- Java Developer Newsletter: From your Oracle account, select **Subscriptions**, expand **Technology**, and subscribe to **Java**
- Java Developer Day hands-on workshops (free) and other events
- Java Magazine

JDK 8u131 checksum

**Java SE Development Kit 8u131**

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

Accept License Agreement  Decline License Agreement

Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	77.87 MB	<a href="#">jdk-8u131-linux-arm32-vfp-hflt.tar.gz</a>
Linux ARM 64 Hard Float ABI	74.81 MB	<a href="#">jdk-8u131-linux-arm64-vfp-hflt.tar.gz</a>
Linux x86	164.66 MB	<a href="#">jdk-8u131-linux-i586.rpm</a>
Linux x86	179.39 MB	<a href="#">jdk-8u131-linux-i586.tar.gz</a>
Linux x64	162.11 MB	<a href="#">jdk-8u131-linux-x64.rpm</a>
Linux x64	176.95 MB	<a href="#">jdk-8u131-linux-x64.tar.gz</a>
Mac OS X	226.57 MB	<a href="#">jdk-8u131-macosx-x64.dmg</a>
Solaris SPARC 64-bit	139.79 MB	<a href="#">jdk-8u131-solaris-sparcv9.tar.Z</a>
Solaris SPARC 64-bit	99.13 MB	<a href="#">jdk-8u131-solaris-sparcv9.tar.gz</a>
Solaris x64	140.51 MB	<a href="#">jdk-8u131-solaris-x64.tar.Z</a>
Solaris x64	96.96 MB	<a href="#">jdk-8u131-solaris-x64.tar.gz</a>
Windows x86	191.22 MB	<a href="#">jdk-8u131-windows-i586.exe</a>
Windows x64	198.03 MB	<a href="#">jdk-8u131-windows-x64.exe</a>

Luego de instalado este software, el sistema está preparado para proceder a la instalación de la aplicación “DS-COD” para la Firma Digital de archivos XML que contienen CODs de ALADI.

## Instalación de aplicación de Firma Digital de COD (DS-COD)

Descargue la última versión de la aplicación **DS-COD** desde el enlace disponible en el menú del sistema de Certificados de Origen en el website de la Entidad.

La descarga copiará en un archivo llamado **“ds-cod-v1.1.0.zip”**. Descomprímalo en una carpeta dentro de su computadora. En la misma se creará una carpeta llamada **“ds-cod”**. Dentro de ella otra carpeta con la versión de la aplicación, por ejemplo **“1.1.0”**. Allí encontrará archivos con extensión **“\*.jar”** (las aplicaciones de firma digital listas para usar desde la línea de comando y una con un front-end gráfico), un manual de usuario en formato PDF y una carpeta **“src”** con el código fuente del sistema.

Una buena idea para empezar es abrir la aplicación **“firmar-gui.jar”** haciendo doble-click sobre la misma y leyendo el manual de usuario.

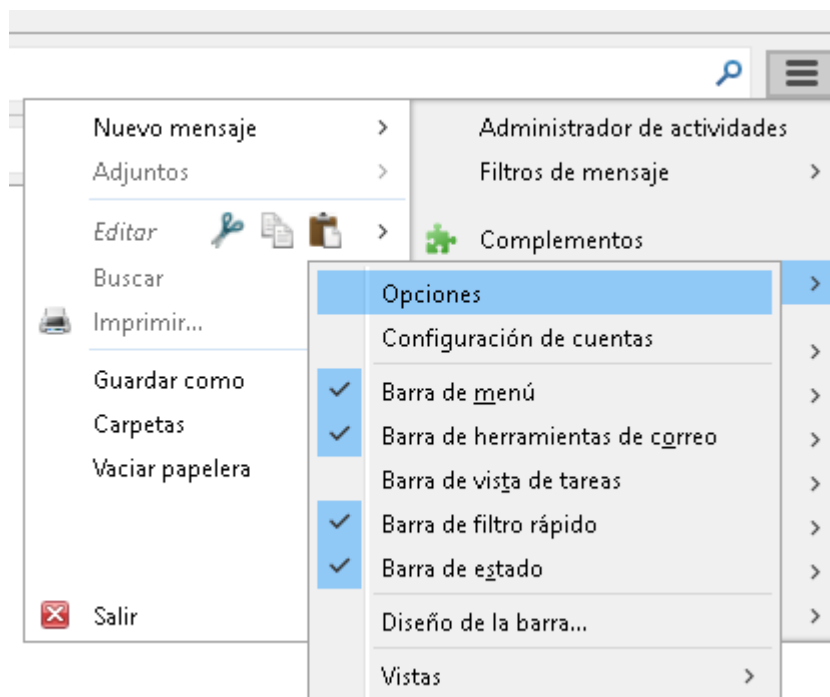
## Instalación de SafeNET iKey 4000 en Mozilla Thunderbird (sólo para entidades y funcionarios)

Los correos electrónicos que envía el sistema **SCOD de ALADI** vienen firmados y cifrados digitalmente con la parte pública del certificado del funcionario que lo recibe (**X.509 v3 con .PEM**). Para poder acceder a su contenido es necesario instalar el driver del dispositivo **SafeNET** en la aplicación **Mozilla Thunderbird**. Esto se realiza siguiendo estos pasos:

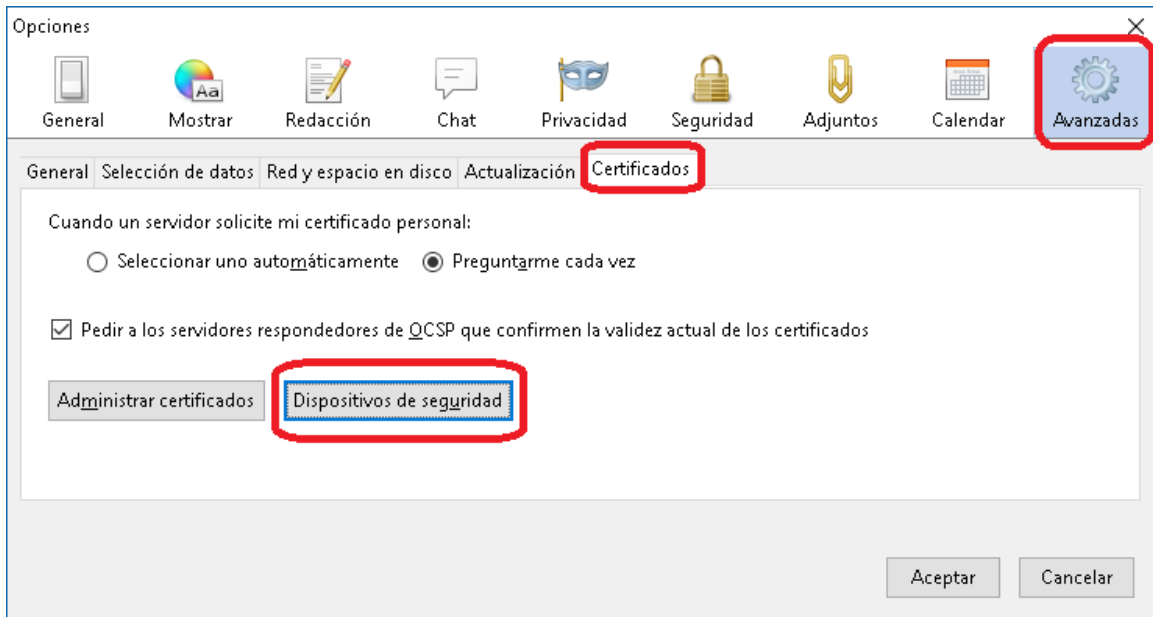
### a) Descargue e instale la aplicación de correo electrónico (no necesita ser administrador del sistema)

<https://www.mozilla.org/es-AR/thunderbird/>

### b) Ejecútelo y acceda al menú de opciones

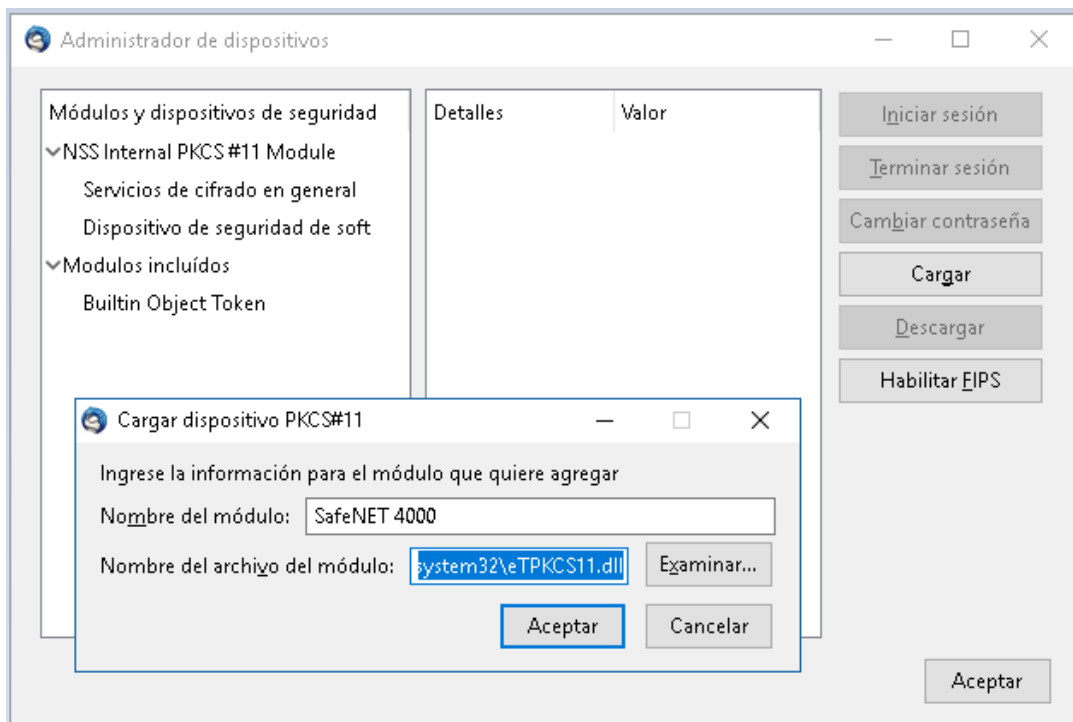


**c) Vaya a “Dispositivos de Seguridad”**



**d) Vaya a “Cargar”, asigne un nombre y coloque la ruta o path en donde está el archivo .DLL con el driver para acceder al mismo**

En caso de Windows lo más común es encontrarlo en “C:\WINDOWS\system32\TPKCS11.dll”



**e) Acepte y cierre todas las ventanas. Cuando llegue un email firmado y cifrado, Mozilla Thunderbir le pedirá la contraseña del token y a partir de allí podrá visualizarlo**

## Descarga del certificado digital (parte pública) de su firma digital: *Certificado X.509 en formato .PEM*

---

El archivo **.PEM** que contiene el certificado **X.509** de un usuario de firma digital, está codificado en caracteres imprimibles (ASCII) en “**base64**”. Este certificado X.509 es emitido por la autoridad certificadora (AC) y contiene una clave pública más una serie de datos que permiten identificar al emisor del mismo. El formato está muy bien explicado en Wikipedia:

<https://es.wikipedia.org/wiki/X.509>

Los sistemas que operan con Certificados de Origen Digital **registran los certificados X.509** de cada uno de los actores en la cadena de firmas. La aplicación **SCOD de ALADI** los registra en formato **.PEM** bajo el nombre de **CID**. **El sistema SCOD sólo registra los CID de los Funcionarios Habilitados (FH) para firmar de cada una de las Entidades (EH) de cada país miembro.**

Por otra parte, las Entidades Habilitadas (**EH**) agregan a su registro de firmas habitual el certificado digital en formato **.PEM** de cada uno de ellos. Ahora este registro de firmas contendrá cada CID de cada firma autorizada de cada exportador para nutrirse de la naturaleza que la firma digital impone (fechas válidas, autoridad certificante y similares). El registro de firmas de la entidad tendrá esta información adicional, además de la clásica, tal como ficha con firma caligráfica, sellos, poderes habilitantes o los estatutos de las empresas.

**Los Funcionarios Habilitados (FH) deben registrar su .PEM en SCOD de ALADI. Los Exportadores harán lo propio en el sistemas informático de cada Entidad Habilitada (EH).**

En caso de la Firma Digital provista por la **AC de AFIP**, el usuario debe ingresar al portal con su CUIT/CUIL y Contraseña. Luego debe ir a la sección “**AC de AFIP**” y a partir de allí consultar su Firma Digital y exportar o descargarse su archivo **.PEM**