



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 legalmentre 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 ingún 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 **distrubición 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 verisón 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.

SafeNey IKey ComPlus 🔹	✓ ³ B	Buscar en 🔎			
Nombre	Fecha de modificación	Tipo	Tamaño		
🔀 sac10-x32.msi	28/4/2017 11:19 p. m.	Paquete de Windows Installer	9,5 0 4 KB		
🔀 sac10-x64.msi	28/4/2017 11:19 p. m.	Paquete de Windows Installer	12,626 KB		







Una vez concluída 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.

	SafeNet Authentication Client Tools	×
📱 Información del dispositivo:	×	gemalto
SafeNet Authentication Clier	t gemalto	ion Client 🛛 🔿 👩 🛔 🤋 🏚
Nombre del dispositivo Cetegoria del dispositivo	Hadasae	
Nondre de lactor Número de serie Capacidad totel de la memoria Econolis Rico de la transfa del decosition	Rainbow Technologies Key/VituaReader 0 0x89128543 73720 50730	Cambiar nontitre al dispositivo
Arción de hardware Arción de hardware Arción de fanware Di de la neutra	08 10 89129543	Cambiar Contraceña del depositivo
Nombre del producto Nodelo Too de tarietà	Kay 4000 SafeVer M 400 SCCDS	Dellingue digodos
Vernión del SO Versión de máncara Colos	SCCDS V10 N/A N/A	Elminar contenido del dispositivo
Tanvaño de clave admitido Contraseña del depositivo Número de reintentos restantes de la Contraseña del dirpo	2048 bits Presente tivo: 10	Ver información del dispositivo
Número máximo de reintentos de la Contraceño del dispositivo Cierre de sesión autoristico del dispositivo	10 Tracle inactivided del dispositivo: en minutos: 10 V Copier OK	Oscoolectal Salattile al osav What
SafeN		GEMALTO.COM
SateNer Au Copyright Reservedo	Abentication Client 10.0 (10.0 43.0) 9 2015 SafeNet, Inc. <u>Intra //www.safemet-inc.com/</u> 1 todos los derechos.	
Informació Fecha de Licencia d	n de licencia licencia: Thu Apr 10 13 52:37 2014 concedida a: Adrenistración Federal de Ingresos: Publicos (AFIP), 7 Ingostar nuevo licencia	2504
	OK	
3 9		





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 Kir 🛛 🛪						- an	and a the				
- C 🛈 www.orade.c	om/technetwork/java/javase/downloa	ds/jtlk8-downloads-2133	IS1.html	« I	Å.	0 9		0 🔳	13 5	Э	
	Sign In/Register Help Country ~ (Products Solutions Dov Iava - Java 8E - Downloads	Communities ∽ I am a ∽ vriloads Store Su	lwantto∽ Ipport Tra	Sear	ch Partner	Q s Ab	out [OTN			
										2	
Java SE	Overview Downloads Docum	entation Community T	echnologies	Training			Java SD	Ks and 1	loois		
Java EE	The second		and his second stall			1 ± 1	ava SE				
Jova ME	Java CE Douglanman	Vit 0 Deumlanda				* 1	ava EE a	nd Glass	fish		
Java SE Summet	Thank you for development	are of the locaTH Distform	Standard Edition	Developm	ant Mit	- 1	Java ME				
terre de l'algorithe de	(JDK ^{**}) The JDK is a development	t environment for building ap	plications, apple	its and	ene est						
ravia 20 withsuced 9 2nde	components using the Java progra	mming language				24	ava caro	2003			
Java Enibedded	The IDM includes tools useful for a	leveloping and testing progra	man written in the	a lawa		- L	NetBeans IDE				
Java DB	programming language and running	The JDK includes tools useful for developing and testing programs written in the Java programming language and supplied on the Java platform.						💂 Java Mission Control			
Web Ter	Page along	and a second second second second					Java Resources Java APIs Technical Articles				
Java Card	 See also: Leve Developer Newslatter: Fr 	om vour Oracla account sale	- Subscription-	e ovrond							
Java TV	Technology, and subscribe to	Java	set onion centrations	e, expand		•					
Neurite Jour	 Java Developer Day hands-on 	workshops (hee) and other	events			• I					
new to save	- Java Manatina					. ₽	Demos and Videos Forums				
connunty	 Java magazine 					₽ E					
Java Magazine	JDK 8u131 checksum						ava Maga	zine			
							ave col	ALC: NO			
	Java S	E Development K	it 811131			* 1	avanes	An teach			
	You must accent the Oracle Bi	any Code Linense Anreeme	ent for Jana SE to	n download	this	1 L	eveloper	Training	Ę.		
	the mine decept the crucic th	software.	in the book be t	o aominio		± 1	utorials				
	Accept Lice	nse Agreement 👘 Declin	e License Agre	ement		÷ .]	ava.com				
	Product / File Description	File Size	Download	L. C.							
	Linux ARM 32 Hard Float ABI	77.87 MB 🛓 dk-8u131	anui-arm32-sfp	-hill.tar.gz							
	Linux ARM 64 Hard Float ABI	74.81 MB +idk-8u1.31	linux-arm64-vfp	-hftttar.gz							
	Linux iss	164.66 MB 90%-00131-	snuk 1566 rpm								
	Linux x86	1/3/38 MB 106-80131-	angue 1986 sar gz								
	Linux s64	176.95 MB	linine x64 tar az								
	Mac OS X	226.57 MB +idk-But 31-	macosx-x64 dm	na							
	Solaris SPARC 64-bit	13979 MB Hidk-8u131	solaris-sparcy9	tar.Z							
	Solaris SPARC 64-bit	99.13 MB + dk-6u131-	evans-sparcv9	tar.gz							
	Solaris x64	140.51 MB 🛓dk-Bu131-	solaris x84,tar.2	1							
	Solaris x64	96.96 MB 10k-6u131	-solaris-x64.tar g	12							
	Windows x96	191.22 MB 104-8u131	windows-i596.e	308							
	Windows x64	198.03 MB 10k-6u131	windows-x64 as	18							

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 dispositvo **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"

Opciones								×
	Aa		=	90		Q		Ę
General	Mostrar	Redacción	Chat	Privacidad	Seguridad	Adjuntos	Calendar	Avanzadas
General Sele	cción de datos	Red y espacio en	disco Actua	alización Certific	ados			
Cuando ur	n servidor solici	te mi certificado p	ersonal:					
O Se	leccionar uno a	iutomáticamente	Pregun	itarme cada vez				
Ŭ		-	0.0	-				
🗹 Pedira	los servidores	respondedores de	<u>O</u> CSP que co	onfirmen la valid	ez actual de los	certificados		
				a				
Ad <u>m</u> inist	Ad <u>m</u> inistrar certificados Dispositivos de seg <u>u</u> ridad							
							Acontax	Concelor
							Acchar	Cancelar

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\eTPKCS11.dll"

Administrador de dispositivos	- 🗆 ×
Módulos y dispositivos de seguridad VNSS Internal PKCS #11 Module Servicios de cifrado en general Dispositivo de seguridad de soft VModulos incluídos Builtin Object Token	I <u>n</u> iciar sesión Terminar sesión Cam <u>b</u> iar contraseña Cargar
Cargar dispositivo PKCS#11 — X Ingrese la información para el módulo que quiere agregar	<u>D</u> escargar Habilitar <u>F</u> IPS
No <u>m</u> bre del módulo: SafeNET 4000 Nombre del archi <u>v</u> o del módulo: <mark>system32\eTPKCS11.dll</mark> E <u>x</u> aminar Aceptar Cancelar	Aceptar

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