Instrucciones abreviadas para la configuración de la Firma Electrónica

Autor: Javier Batista
Versión del documento: 0.1

1. Descargar los 3 certificados de las Autoridades de Certificación de Panamá (**caraiz, cagob** y **capc2)** en la siguiente dirección: http://www.pki.gob.pa/cert.htm . **Opcionalmente** los mismos se pueden importar en el sistema operativo (Windows o macOS) para que sean reconocidos por otros programas diferentes al Adobe Reader (para mayor referencia se pueden revisar los manuales de configuración en http://www.pki.gob.pa/drivers.htm).

2. Instalar el driver de **SafeSign** de la tarjeta correspondiente a su sistema operativo: http://www.pki.gob.pa/drivers.htm . Si es Windows, puede utilizar **SafeSign Identity Client 3.0.112 - Windows 10** (http://www.pki.gob.pa/drivers/SafeSignIC30112-x64-win-tu-admin.exe) o en el caso de **macOS**, se debe descargar **SafeSign Identity Client 3.0.72 - Mac OS X x64** (http://www.pki.gob.pa/drivers/SafeSign_Identity_Client-Standard-3.0.72-general-i386-x86_64.zip). Cuando se finalice la instalación, se incluirá un programa llamado **Administración de tokens** (se puede buscar escribiendo **tokenadmin** en el menú de inicio de **Windows** o en el **Launchpad** de **macOS**); donde si se conecta la tarjeta con el lector USB en la computadora, deberá aparecer su cédula con el estado de operativo en dicho programa.

3. Para firmar un documento en el programa **Adobe Acrobat Reader DC** (si no lo tiene instalado se puede descargar en https://get.adobe.com/es/reader/), se deben importar los 3 certificados de las CA (http://www.pki.gob.pa/cert.htm), descargados en el primer paso, con sus permisos en la opción de **Edición -> Preferencias -> Firmas -> Identidades y certificados de confianza** (tercer botón de **Más**) **-> Certificados de Confianza -> Importar** (flecha azul invertida y si es **macOS**, la opción de **Preferencias** está en **Acrobat Reader**). Se agrega primero el certificado raíz (**caraiz**) con el botón de **Examinar** en la ventana **Elegir contactos para importar**, luego cuando aparece el nombre "**AUTORIDAD CERTIFICADORA DE PANAMA**", se selecciona tanto en **Contactos** como en **Certificados**, luego se usa el botón de **Confiar,** marcando todas las casillas, empezando con "**Utilizar este certificado como raíz de confianza**" hasta la última. Luego se agregan los otros dos certificados (**cagob** y **capc2**) importándolos directamente con la misma opción (pero sin usar el botón de **Confiar**) y deberían heredar toda la confianza de la raíz (todos lo ganchos menos el primero de raíz de confianza).

4. Luego se debe asociar la librería del driver de la tarjeta en el Adobe Reader, donde en el caso de **Windows** deberá ir a la opción de **Edición -> Preferencias -> Seguridad (mejorada)** y desmarcar la opción **Activar modo protegido al iniciar**, reinicia el Adobe (saliendo y volviendo a entrar), para ir nuevamente a **Edición -> Preferencias -> Firmas -> Identidades y certificados de confianza** (tercer botón de más), luego entra en **ID digitales -> Módulos y distintivos PKCS#11**, allí debería estar habilitado el botón

de **Adjuntar módulo**, se presiona y deberá buscar el archivo DLL llamado **aetpkss1.dll** en la carpeta **C:\Windows\SysWOW64** en caso de que la versión de Windows sea 64 bits o la ruta **C:\Windows\System32** si su sistema operativo es de 32 bits. Si es **macOS**, se copia solamente la ruta **/usr/local/lib/libaetpkss.dylib** al presionar el botón de **Adjuntar módulo.** Luego nos dirigimos a **Módulos y distintivos PKCS#11 -> Cryptographic Token Interface -> Iniciar sesión**, se coloca el número PIN de la tarjeta y debajo de **Cryptographic Token Interface** aparecerá su cédula, se selecciona y luego en pantalla saldrán los dos certificados ([A] NOMBRE... y [F] NOMBRE...), se marca el de **[F] NOMBRE...** y se da click en el icono del lápiz superior **Opciones de uso -> Usar para firmar**, donde quedará un ícono de un bolígrafo por delante del certificado utilizado para firmar ([F] NOMBRE...), luego se cierra esa ventana pero nos mantenemos en la de **Preferencias**.

5. Se debe agregar la dirección del servidor de sellado de tiempo en **Edición -> Preferencias -> Firmas -> Marca de hora del documento** (cuarto botón de **Más**) **-> Servidores de marca de hora -> Nuevo** (icono de + azul). En el campo **Nombre** se puede colocar: **TSA de Panamá** y en **Dirección URL del Servidor:** http://tsp.pki.gob.pa/ , se presiona **Aceptar**; luego se da click en **Establecer predeterminado** (icono de la estrella) y el botón de **Aceptar,** para que el servidor de la marca de hora esté por defecto, ya que será utilizado cada vez que se firme un documento.

6. Para firmar siempre se usará la opción de **Herramientas -> Certificados -> Firmar digitalmente**, se dibuja el cuadro de la imagen de la firma con el tamaño deseado en cualquier parte del documento con un espacio vacío. Luego debe estar seleccionado el certificado que empieza con **[F] NOMBRE...** se da click en **Continuar** -> **Firmar** (en esta ventana se debe pedir el número PIN, pero si se inició sesión previamente en **Preferencias** ya no lo pedirá al menos que se reinicie el Adobe). Después de presionar el botón de **Firmar**, se guarda el documento como uno nuevo (cambiándole el nombre o guardándolo en otra carpeta para no sobrescribir el original) y la primera vez se notificará que se está estableciendo conexión con el servidor de sellado de tiempo http://tsp.pki.gob.pa/ y se presiona el botón de **Permitir**, verificando que recuerde la acción para evitar que el mensaje vuelva aparecer. Al final debe quedar la imagen de la firma en el documento y si se da click en ella, aparecerá una ventana indicando que la firma es válida; también debe aparecer una barra celeste en la parte superior del documento con el mensaje: "**Firmado y todas las firmas son válidas**", pero si la barra no aparece la primera vez, se puede cerrar y abrir nuevamente el documento firmado, donde sí debería salir dicho mensaje. Con este paso, el **Adobe Reade**r ya está configurado correctamente para firmar documentos.