Hacienda

Firma digital guía de uso de certificados y firma digital

Versión 7.0

29 de julio de 2024

TABLA DE CONTENIDO

1 OBJETIVO DE LA GUIA

El objetivo de este documento es contextualizar al usuario del SIIF Nación acerca del uso del certificado y la firma digital en el SIIF Nación.

2 ALCANCE

Con el uso de esta guía el usuario del SIIF Nación conocerá acerca de la firma y certificados digitales en su concepto y base legal, así como utilizarla en las funcionalidades del SIIF Nación que así lo requieran.

3 TÉRMINOS Y DEFINICIONES

- **Certificado digital:** Los certificados digitales son documentos digitales emitidos a una persona natural o jurídica, que contiene datos propios de la persona o empresa, que son validados por quien emite el certificado.

  El certificado digital se puede asimilar a los documentos emitidos por entidades autorizadas mediante los cuales nos identificamos, tales como el documento de Identidad emitido por la Registraduría, o un carné emitido por una empresa.

  El Certificado digital sirve para identificarse ante terceros, y mitiga la suplantación de la identidad en Sistemas de Información.

- **Certificado digital centralizado:** Agrupación de certificados digitales en un único sitio seguro para su administración y uso. En el SIIF Nación, se puede utilizar certificados digitales centralizados o almacenados en token criptográfico.

- **Firma digital:** La ley 527 de 1999, la define en el artículo 2 numeral c), "Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido,

vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

- **Token criptográfico**: Dispositivo físico donde se almacena el certificado digital de función pública del usuario.

4 CONDICIONES ESPECIALES PARA LA OPERACIÓN DE LA GUIA

Para el correcto uso de certificados digitales en el aplicativo SIIF Nación, es necesario tener instalado previamente el componente cliente para la firma digital y el controlador o driver del dispositivo de almacenamiento criptográfico (token) o de certificados centralizados en su computador.

Estos procedimientos deben ser realizados por el personal de soporte técnico de la entidad usuaria y con permisos de Administración sobre el computador que utiliza el usuario SIIF Nación.

5 DOCUMENTOS RELACIONADOS

- Guía de instalación prerrequisitos para el uso de certificados digitales en SIIF Nación.

  Dirigido al soporte técnico de la entidad, en la cual se indica los componentes que se deben instalar en el computador del usuario previo al uso de la firma digital.

- Reglamento de uso del SIIF Nación.

  Dirigido al usuario final, se establecen normas de obligatorio cumplimiento por parte del usuario sobre la utilización del SIIF Nación.

- Recomendaciones de seguridad del SIIF Nación.

Dirigido al usuario final, contiene indicaciones a tener en cuenta para el uso seguro del SIIF Nación.

6 BASE LEGAL

- Decreto 1068 de 2015 parte 9. Mediante el cual se reglamenta el SIIF Nación.
- Ley 527 de 1999. "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."
- Decreto 1747 de 2000 "Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales".
- Decreto 333 DE 2014 Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012.

  Decreto que tiene por objeto "definir el régimen de acreditación de las entidades de certificación, en desarrollo de lo previsto en el artículo 160 del Decreto ley 19 de 2012"

7 USO DE CERTIFICADOS Y FIRMA DIGITAL EN EL SIIF NACION

En Colombia, la emisión del certificado digital está bajo la responsabilidad de una entidad de certificación debidamente acreditada por el Organismo Nacional de Acreditación de Colombia - ONAC (Ley 527 art. 29-34, decreto 333 de 2014 art. 7)., así mismo en dicha ley se establece el reconocimiento jurídico de los

mensajes de datos y de la firma digital[1], teniendo la firma digital la misma fuerza y efectos que el uso de una firma manuscrita (Ley 527 art.28).

En el aplicativo SIIF Nación, el certificado digital es utilizado para identificar el usuario que ingresa al sistema, firmar digitalmente aquellas transacciones que son sensibles para la seguridad del sistema, permitiendo identificar a la persona que realiza los registros en el aplicativo, garantizar la integridad[2] y no repudio[3] de los datos que registra.

Se utiliza el certificado digital almacenado en un dispositivo criptográfico[4] (token) o centralizados, provistos por las entidades de certificación autorizadas por la ONAC y homologadas por la Administración del SIIF Nación, para firmar digitalmente las funcionalidades[5] que la Administración SIIF Nación establece como requisito para ser registradas o modificadas; así como para firmar los archivos utilizados para las cargas masivas de datos.

Es responsabilidad del usuario el uso adecuado que se le dé al certificado digital utilizado para firmar digitalmente. El certificado

1 La ley 527 de 1999, define en el artículo 2 numeral c), Firma digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

2 La ley 527 de 1999, define en el artículo 9 Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

3 No repudio: Quien realizó los registros no lo puede negar. La identidad se establece a través del certificado digital utilizado para firmar digitalmente la funcionalidad que exige firma digital.

4 Token: Dispositivo entregado al usuario donde se almacena su certificado digital. El acceso al certificado es protegido por un PIN o contraseña.

5 Funcionalidades que requieren firma digital: Para conocer la lista de funcionalidades que requieren firma digital en el SIIF Nación consultar en el menú de reportes ADM / Transacción / Transacciones del sistema asignando Sí al filtro de "Atributo de alto requerimiento de seguridad".

digital emitido a nombre del usuario, el token criptográfico y su contraseña de acceso (PIN), así como los mecanismos de control de acceso al certificado digital centralizado, son de uso personal e intransferible. Así mismo, el usuario es responsable de solicitar a la entidad de certificación que emitió el certificado su revocación, cuando el usuario deje de requerir el uso del certificado digital, por ejemplo, cuando se retira de la entidad, cuando se pierda o dañe o bloquee el token criptográfico, o por alguno de los motivos establecidos por la entidad de certificación.

Mantenga bajo su custodia el token criptográfico, no lo deje conectado al computador cuando esté ausente, así como para el caso de certificados digitales centralizados, cerrar la sesión cuando no lo esté utilizando.

Importante: Antes de poder firmar digitalmente transacciones en el aplicativo SIIF Nación o realizar cargas masivas de datos, es necesario que el soporte técnico de su entidad haya instalado en su computador los prerrequisitos explicados en la "Guía de instalación prerrequisitos para el uso de certificados digitales en SIIF Nación" mencionada en el numeral 5**¡Error! No se encuentra el origen de la referencia.**.

7.1 Consideraciones iniciales

De otra parte, cuando se presenten actualizaciones de los componentes externos utilizados para la firma digital, se puede presentar un mensaje indicando que hay actualizaciones disponibles, dado que para realizar la actualización se requiere **permisos** de **administración** sobre el computador que se está utilizando, **solicite inmediatamente al soporte técnico de su entidad que realice el proceso de actualización de acuerdo con las políticas de actualización de software que se tengan.**

7.2 Firmar digitalmente una transacción.

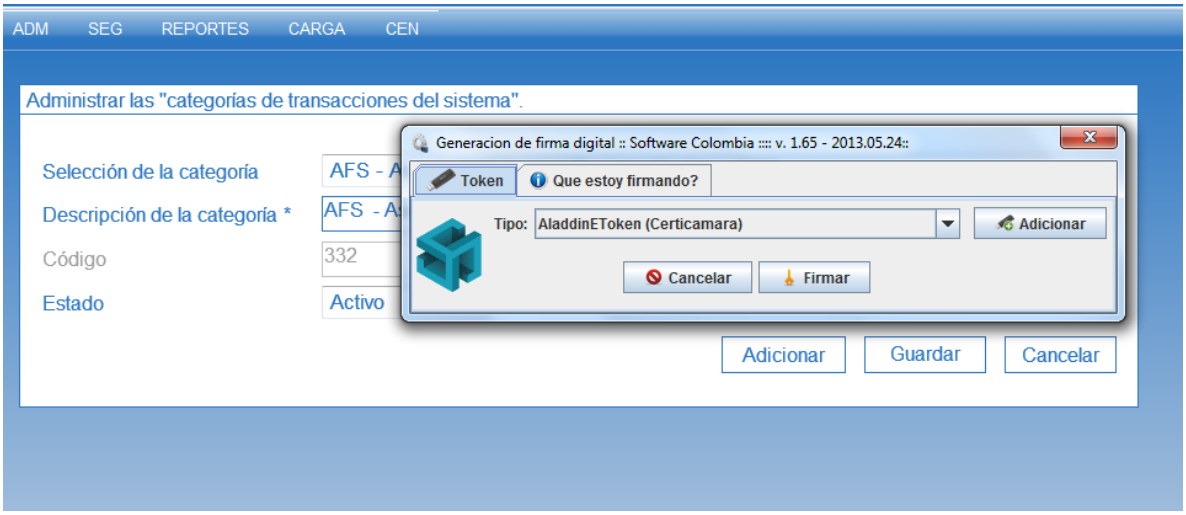
Cuando la transacción que se esté realizando exija firma digital, una vez se utilice el botón para guardar los datos, se va a solicitar la firma digital.

Paso 1:

Importante:

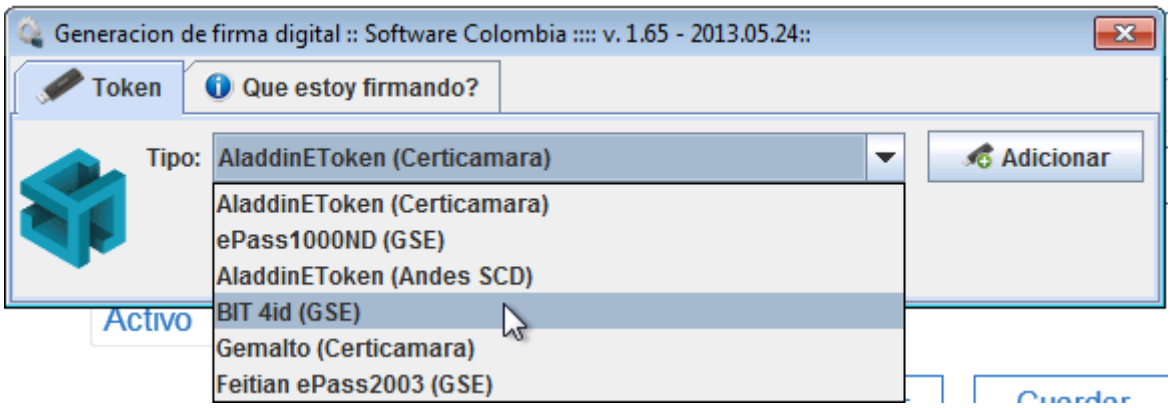
Asegúrese que antes de ingresar al SIIF Nación haya conectado el dispositivo criptográfico Token, en el puerto USB del computador desde el cual va a ingresar; o para el caso de certificados digitales centralizados se haya establecido la sesión de conexión para su uso, según las instrucciones dadas por su proveedor del certificado. De lo contrario se van a presentar fallas cuando intente ingresar al sistema y se intente firmar digitalmente.

Una vez se esté ingresando al sistema y se solicite que se firmen los términos de uso o cualquier otra transacción que solicite firma digital, se muestra la interfaz principal de firma digital en la cual deberá seleccionar la pestaña de firma con certificado almacenado en dispositivo criptográfico (Token). (Esto aplica tanto para certificados digitales almacenados en token criptográfico como centralizados).



Paso 2:

Posteriormente, el usuario deberá seleccionar el tipo de dispositivo criptográfico, sea para el almacenado en token criptográfico o centralizado, en el cual se encuentra almacenado su certificado digital. Por defecto, se encuentra pre-configurado con los siguientes dispositivos soportados por las Entidades de Certificación Digital acreditadas por el Organismo Nacional de Acreditación (Ley 527 art. 29-34).

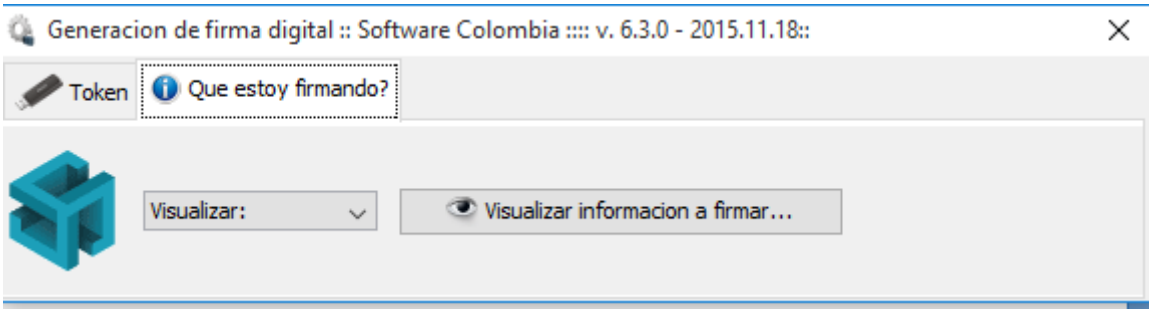


NOTA:

En caso de que no conozca cual dispositivo seleccionar, consulte a la entidad de certificación que expidió el certificado digital.

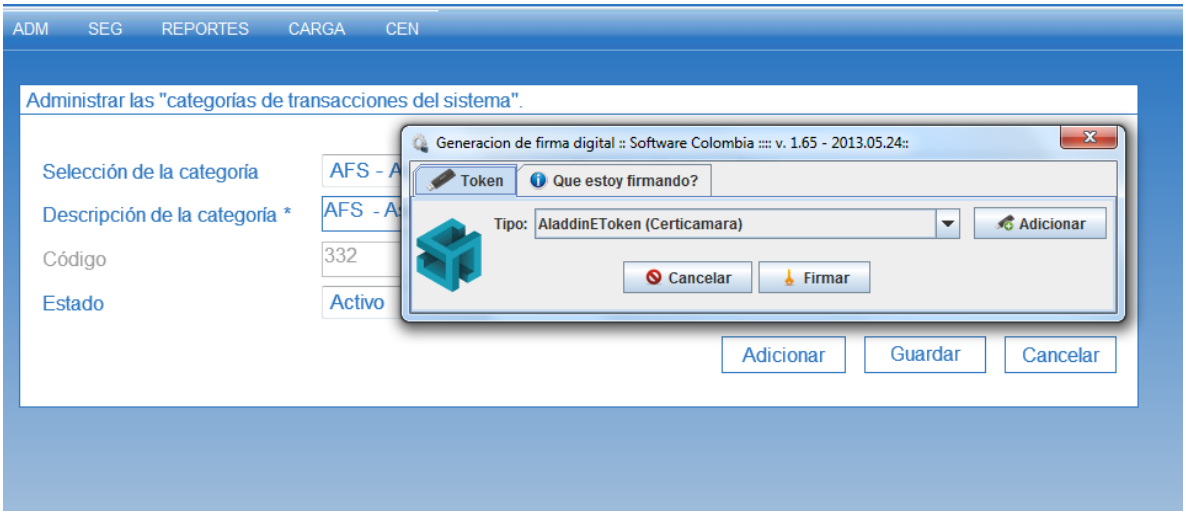
Así mismo, si el tipo de dispositivo no se encuentra en la lista, solicite al soporte técnico de la entidad de certificación ayuda para que utilizando el botón "Adicionar" que se muestra en la imagen inmediatamente anterior se configure el tipo de token criptográfico o dispositivo a utilizar.

Puede ver la imagen del archivo que contiene la evidencia digital, dando clic sobre la pestaña "Que estoy firmando", y posteriormente sobre el botón "Visualizar información a firmar"



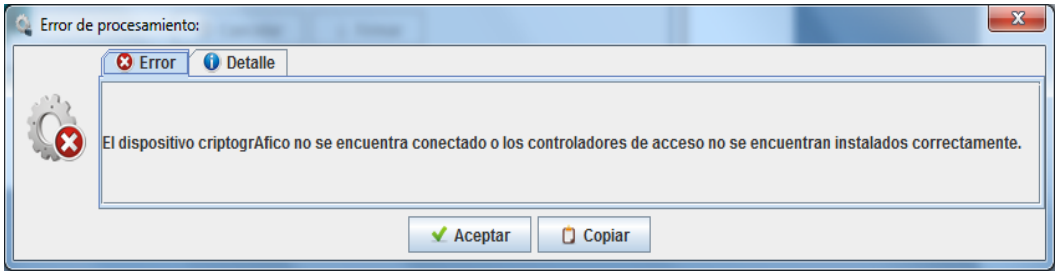
Paso 3:

Después de seleccionar el tipo de dispositivo criptográfico o centralizado, el usuario deberá hacer clic sobre el botón *Firmar*



Recuerde:

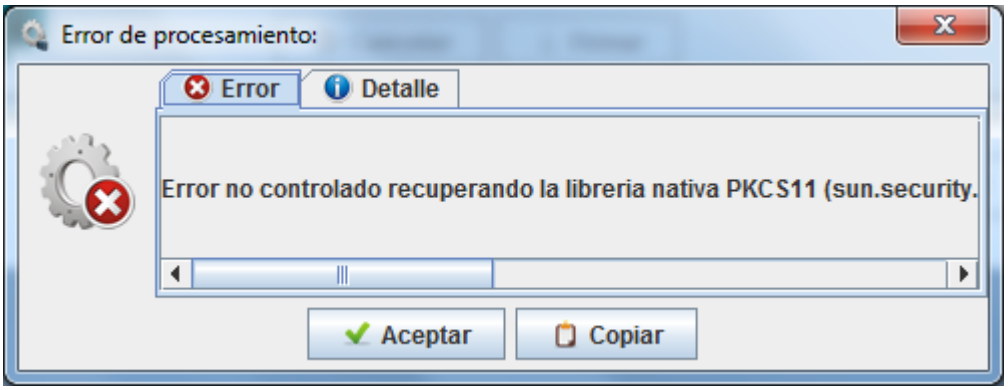
En caso que no se haya instalado los controladores del token o no esté conectado el token al computador que se está utilizando o se esté utilizando certificado digital centralizado y no se haya establecido la sesión de acceso al certificado, se va a mostrar el siguiente mensaje:



En este caso, según corresponda conecte el token o establezca la sesión de conexión al certificado centralizado y vuelva a usar el botón de firmar.

Si persiste el mismo mensaje, solicite al soporte técnico de su entidad que revise según corresponda, que estén instalados los controladores del token o el aplicativo para establecer la sesión de conexión al certificado centralizado, suministrados por la entidad de certificación que expidió el certificado digital.

En caso en el paso anterior no se haya seleccionado el token criptográfico correcto, se va a mostrar alguno de los siguientes mensajes:

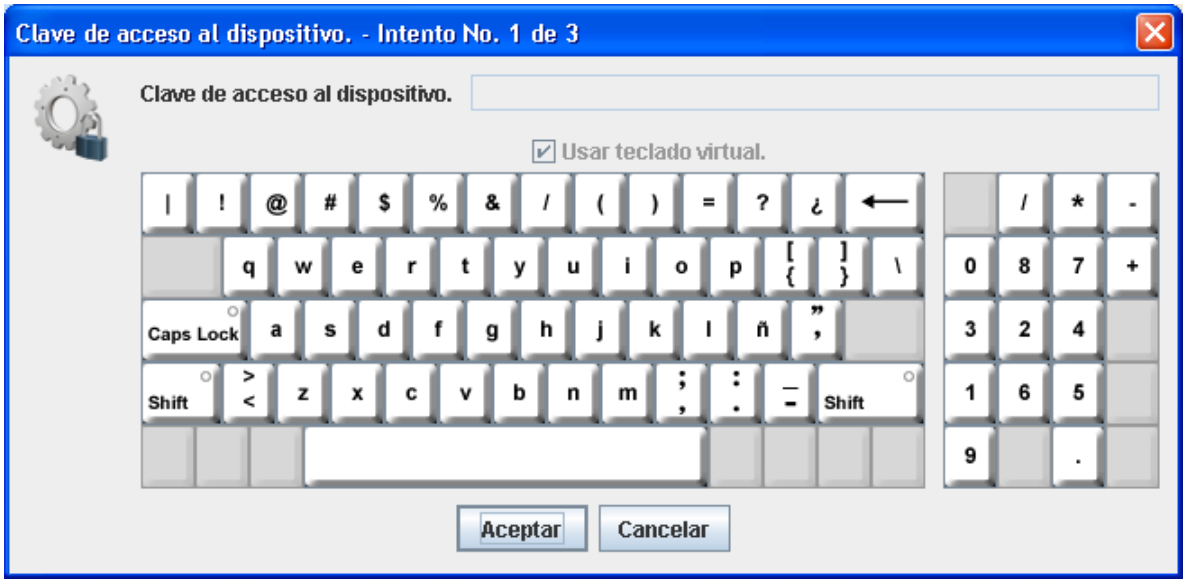


En este caso, selecciónelo de nuevo como se indica en el *paso 2*.

Paso 4:

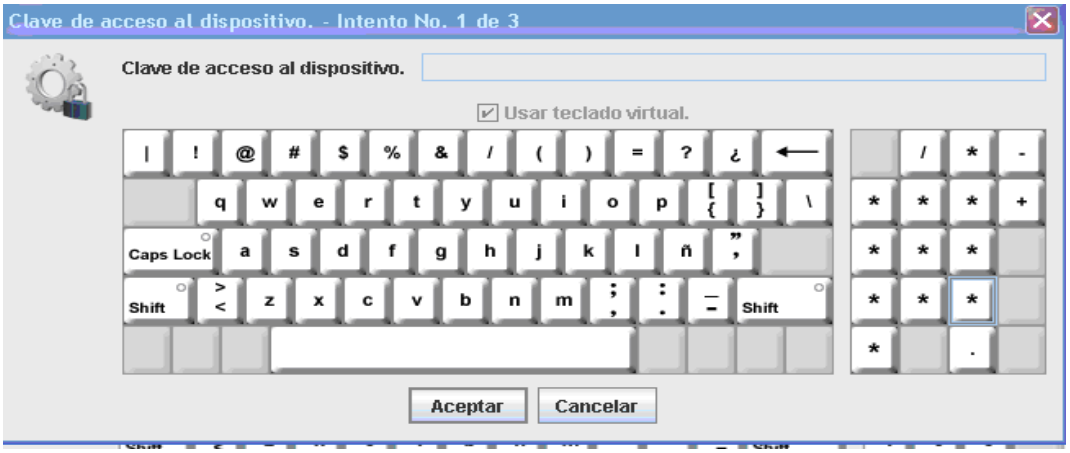
La acción de firma solicitará la clave de acceso al dispositivo criptográfico token.

Es posible que este paso no sea necesario si utiliza certificados digitales centralizados que previamente han solicitado esta clave de acceso.

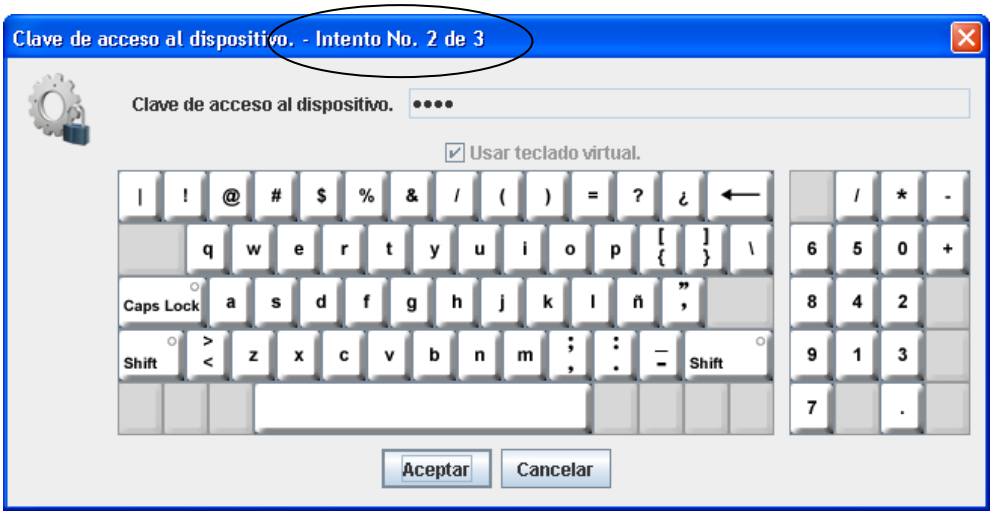


Importante: El teclado numérico se presenta ordenado de manera aleatoria, revisar antes de digitar la contraseña donde se encuentran ubicados los números para digitarlos correctamente. Cuando se acerca el puntero del Mouse al teclado numérico, los números son remplazados por asteriscos.

Si se retira de nuevo el puntero del Mouse del teclado numérico se vuelven a mostrar los números como se ve en la figura anterior.

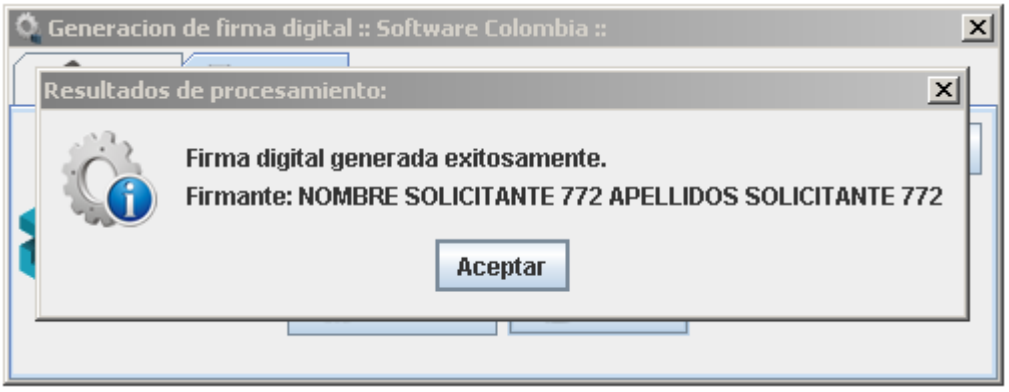


Si la clave de acceso suministrada por el usuario es inválida, se solicitará nuevamente. Sin embargo, se llevará un conteo de los intentos fallidos con el objetivo de evitar el ***bloqueo del dispositivo criptográfico***. Este bloqueo se utiliza como una medida de seguridad contra los atacantes que intentan, a fuerza bruta, conseguir acceso a la llave privada asociada al certificado digital. Es responsabilidad del usuario y de su Entidad de Certificación Digital ejecutar los procedimientos de restablecimiento de contraseñas en caso de bloqueo del dispositivo, en caso de bloqueo del dispositivo criptográfico, puede ser necesaria la adquisición de un nuevo certificado digital.



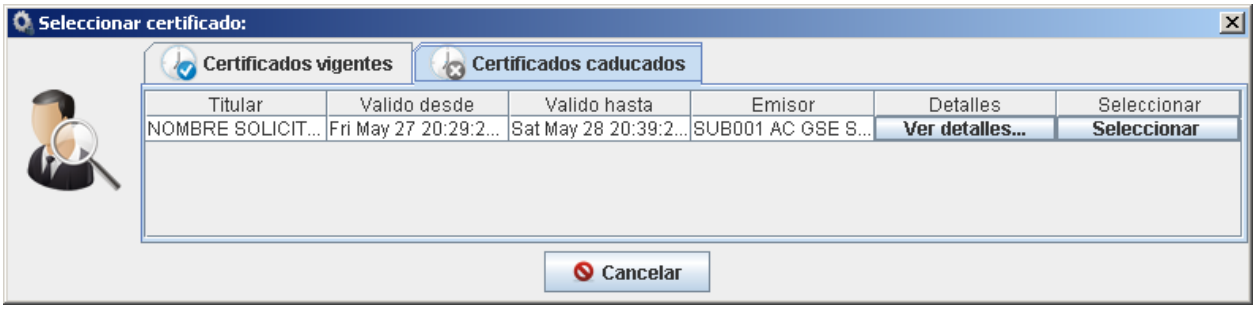
Si la clave de acceso suministrada por el usuario es válida, se procederá a realizar la firma digital.

El sistema finalmente notificará del éxito del cálculo de la firma digital y el nombre del firmante de la transacción.

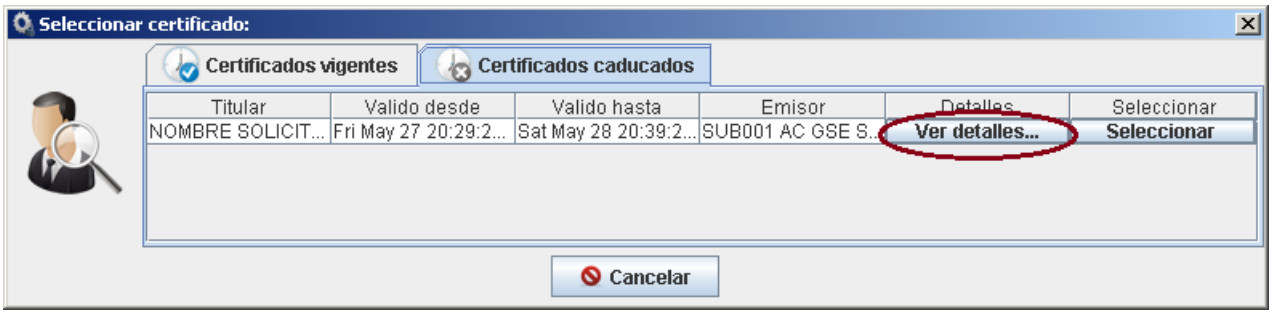


Caso en el cual en el mismo computador o token criptográfico se tiene almacenado más de un certificado digital:

Si la clave de acceso suministrada por el usuario es válida y el computador o dispositivo criptográfico contiene más de un certificado digital (o solo contiene certificados caducados), se procederá a desplegar los certificados disponibles organizados en dos pestañas: (i) Certificados Vigentes y (ii) Certificados Caducados.



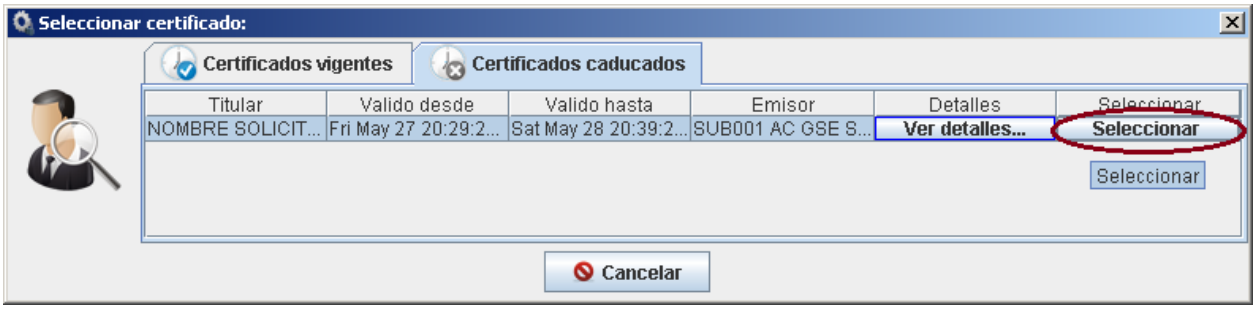
En la lista de certificados desplegados se podrá observar, de primera mano, el titular del certificado digital (campo CN de acuerdo a la especificación X509 V3), su rango de vigencia y la entidad de certificación digital emisora. Si el usuario requiere obtener todos los detalles del certificado digital deberá hacer clic sobre el botón *Ver detalles...*



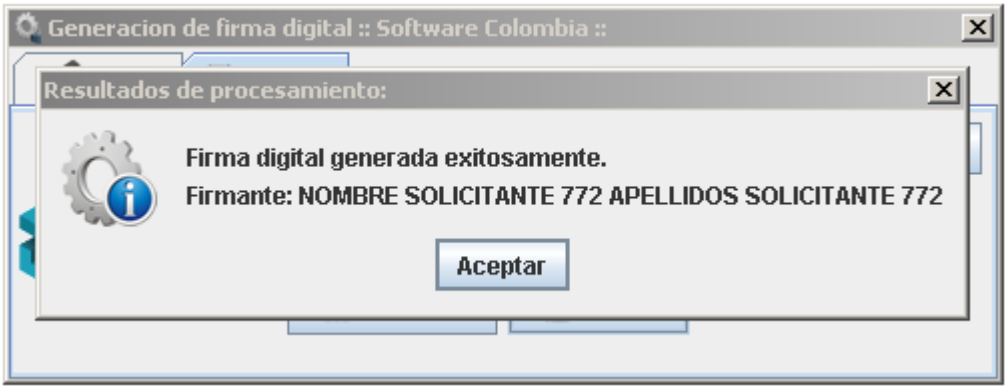
Al momento de hacer clic sobre el botón *Ver detalles...* se desplegará la información disponible en el campo *Asunto (Subject)* del certificado digital X509 V3. La información, si bien presenta propiedades estándares, podrá variar de acuerdo a la entidad de certificación digital emisora. Si el usuario requiere obtener todos los detalles del emisor del certificado digital deberá hacer clic sobre el botón *Detalles emisor...*

Al momento de hacer clic sobre el botón *Detalles emisor...* se desplegará la información disponible en el campo *Emisor (Issuer)* del certificado digital X509 V3. Clic en el botón *Aceptar* para cerrar la ventana de diálogo activa.

Analizada la información desplegada para los certificados disponibles en el dispositivo criptográfico, el usuario deberá seleccionar aquel certificado con el cual se llevarán a cabo los algoritmos de cálculo de firma digital. Esta selección la deberá ejecutar por medio de un clic en el botón *Seleccionar*

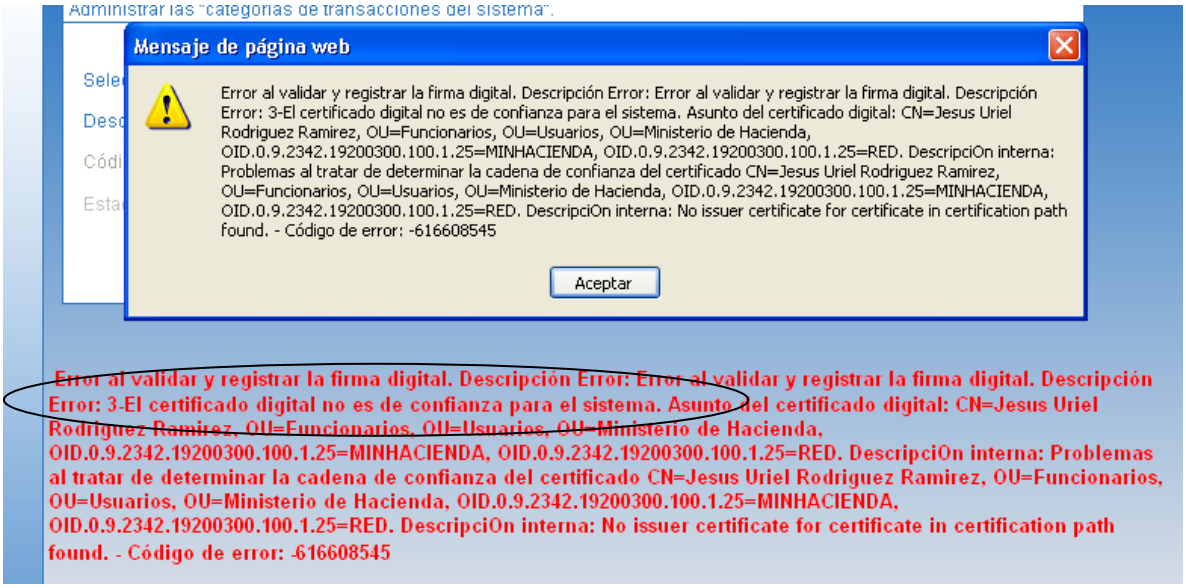


Se notificará del éxito de la firma digital con el siguiente mensaje de diálogo.



Una vez se ha realizado el proceso de firma digital se envía el registro firmado a la base de datos del SIIF Nación, en este proceso se valida que el certificado digital utilizado para firmar sea emitido por una Entidad de Certificación válida para el aplicativo SIIF Nación, que dicho certificado digital esté vigente y que pertenezca al mismo usuario del SIIF Nación. En el caso que no se cumpla con estas validaciones, la transacción no se realiza, sin embargo, se guarda el registro de auditoria de este hecho.

En el siguiente ejemplo se muestra un mensaje de error que se presenta en el caso de utilizar para firmar digitalmente un certificado que no es emitido por una entidad de certificación válida para el SIIF Nación.



Como se señala arriba en la imagen, en este caso en la descripción del error se va a mostrar el texto "El certificado digital no es de confianza para el sistema".

De la misma manera como se muestra arriba, se pueden presentar mensajes de error cuando el certificado digital está revocado o caducado, así mismo se puede presentar un mensaje de error cuando el número de cédula que está en el certificado no es el mismo número de cédula del usuario que está registrado en el SIIF Nación.

De llegar a presentarse al momento de firmar digitalmente un mensaje de error diferente a los indicados en esta guía, solicite al soporte técnico de la entidad que revise la "Guía de problemas frecuentes en el uso de certificados digitales en SIIF Nación".

8 SOPORTE

En caso de requerir soporte en la instalación y manejo de certificados digitales almacenados en token criptográficos, o de certificados digitales centralizados, o firma de archivos para carga masiva, por favor dirigirse al soporte técnico de su entidad o de la entidad de certificación que expidió el certificado digital, o al Coordinador SIIF Nación de su entidad para trámites relacionados con certificados digitales nuevos, caducados o revocados.

9 HISTORIAL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO	AUTOR
2018-10-18	5.1	Actualización nueva versión de componente de firma.	Jesús Uriel Rodríguez Ramírez.
2022-10-18	5.2	Ajustar última actualización para uso de certificados centralizados.	Jesús Uriel Rodríguez Ramírez.
2023-09-21	6.0	Actualización línea gráfica y contenido. .	Jesús Uriel Rodríguez Ramírez.
2024-07-29	7.0	Se actualiza línea gráfica y contenido.	Jesús Uriel Rodríguez Ramírez.

RECUERDE:

En caso de requerir soporte adicional sobre el uso del sistema debe comunicarse a la línea de soporte del SIIF Nación.

Hacienda

Ministerio de Hacienda y Crédito Público

Dirección: Carrera 8 No. 6C–38, Bogotá D.C., Colombia

Conmutador: (+57) 601 3 81 17 00

Línea Gratuita: (+57) 01 8000 910071

Correo: relacionciudadano@minhacienda.gov.co