SISTEMA INTEGRADO DE INFORMACION FINANCIERA SIIF NACION
CIRCULAR EXTERNA No. 002

2.0.0.1

Bogotá D. C., 25 de enero de 2021

PARA: **COORDINADORES DEL SIIF NACION**

ASUNTO: Firma digital en el aplicativo SIIF Nación

La Administración SIIF Nación implementó el uso de la firma digital con base en la ley 527 de 1999, para el registro por parte de los usuarios del aplicativo de transacciones en el SIIF Nación desde el año 2005, utilizando certificados digitales de función pública expedidos por Entidades de Certificación Digital Abierta.

Considerando que el Ministerio de Hacienda - SIIF Nación no es el responsable de la emisión de los certificados digitales, a continuación, se establecen las condiciones para operar con entidades certificadoras digitales abiertas de confianza para el SIIF Nación:

1. La entidad de certificación digital abierta debe estar autorizada por el Organismo Nacional de Acreditación de Colombia – ONAC, para expedir certificados digitales de Función Pública.

2. La entidad de certificación digital abierta debe estar autorizada por la Administración SIIF Nación para utilizar sus certificados digitales de función pública en el aplicativo SIIF Nación almacenados en token criptográfico o almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital.

   Dicha autorización se emitirá por la Administración SIIF Nación, previa solicitud del representante legal a la administración SIIF Nación en la cual se manifieste el cumplimiento de lo establecido en este documento y adjuntando los respectivos documentos soporte y una vez realizadas las pruebas técnicas de funcionamiento de los certificados digitales con el aplicativo SIIF Nación.

   La lista de entidades de certificación digital abierta autorizadas y el tipo de almacenamiento utilizado para el certificado digital autorizado por la Administración del SIIF Nación, puede ser consultada en la página WEB del Ministerio de Hacienda y Crédito Público en www.minhacienda.gov.co / SIIF Sistema Integrado de Información Financiera / Ciclo de Negocios / Administración de seguridad.

3. Los certificados de función pública a utilizar en el SIIF Nación que estén almacenados en Token Criptográficos, estos deben soportar interfaz PKCS11 y cumplir mínimo con el estándar 140-2 Nivel 3 de aseguramiento criptográfico.

4. La entidad de certificación digital abierta debe proveer a sus suscriptores que utilicen token criptográfico, los controladores o drivers para el token criptográfico en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación.

5. Para los certificados de función pública que estén almacenados en un servidor seguro (HSM) provisto por la entidad de certificación digital, la entidad de certificación digital debe proveer a sus suscriptores los controladores o driver para acceder al certificado digital del suscriptor. Este controlador o driver debe cumplir mínimo con:

    a. Integrarse con el terminador de VPN para acceso al SIIF Nación y con el componente cliente de firma digital del SIIF Nación.
    b. Implementar doble factor de autenticación del usuario para acceder al certificado digital almacenado en el servidor seguro (HSM) provisto por la entidad.

6. Los certificados digitales a utilizar en el aplicativo SIIF Nación para sus usuarios, son certificados de Función Pública con estándar X.509.V3, Los certificados deben cumplir con los requisitos exigidos en artículo 35 de la ley 527 de 1999, teniendo en cuenta las siguientes características del certificado digital requeridos en el SIIF Nación:

    a) Nombre
    b) Correo electrónico
    c) Ciudad
    d) Entidad
    e) Cédula de Ciudadanía
    f) NIT de la entidad usuaria
    g) Título o cargo del usuario.
    h) El certificado digital debe utilizar algoritmo de firma: SHA2RSA

7. Los certificados digitales de función pública se deben poder utilizar en el SIIF Nación para:

    a) Autenticación, utilizando un terminador de VPN para acceso al SIIF Nación, el cual verifica la información del certificado y la autorización del SIIF Nación de la entidad de certificación.
    b) Firmar digitalmente transacciones.
    c) Firmar digitalmente archivos para ser utilizados en cargas masivas en el SIIF Nación.

d) El aplicativo SIIF Nación no provee la herramienta para la firma de archivos. La entidad de certificación debe proveer el soporte para el uso de los certificados digitales para la firma de archivos o documentos electrónicos.

8. La entidad de certificación digital abierta deberá proveer a la Administración SIIF Nación, para la validación del estado de revocación del certificado, la publicación de la CRL, adicionalmente el SIIF Nación utilizará el método de verificación del estado del certificado llamado OCSP, para la cual la entidad de certificación digital abierta deberá proveer una URL de acceso a este servicio.

   Cualquier cambio de alguno de estos datos debe ser informado previamente por la entidad de certificación abierta a la administración SIIF Nación.

   Una vez la Administración SIIF Nación informe que dichos cambios fueron aplicados, podrán ser utilizados en el aplicativo SIIF Nación.

9. La entidad de certificación digital abierta debe garantizar, la actualización de la CRL, siendo su responsabilidad que sea oportuna y que esté disponible para consulta durante 7 x 24 x 365 días.

   La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la actualización o disponibilidad de la CRL, dicha responsabilidad recae directamente sobre la entidad certificadora digital abierta.

10. La entidad de certificación digital abierta debe garantizar la disponibilidad del servicio OCSP, siendo su responsabilidad que sea oportuno y que esté disponible para consulta durante 7 x 24 x 365 días.

    La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo que no pueda realizar registros oportunamente por fallas en la disponibilidad del servicio OCSP, dicha responsabilidad recae directamente sobre la entidad de certificación digital abierta.

11. La entidad de certificación digital abierta deberá disponer de la infraestructura de operación, servicio y soporte a sus usuarios, según los acuerdos de niveles de servicio que tenga con la entidad usuaria.

    La administración SIIF Nación no se hace responsable por los perjuicios que pueda ocasionar al usuario del aplicativo las posibles fallas que afecten la operación, servicio o soporte de los usuarios de la entidad de certificación digital abierta.

12. La entidad de certificación digital abierta deberá notificar por lo menos con un mes de anticipación la fecha de vencimiento del certificado digital, así mismo ofrecer al coordinador SIIF Nación de la entidad las herramientas para la gestión (fechas de emisión, fechas de caducidad, cupo utilizado) para una oportuna gestión por parte de este de los certificados digitales. Así mismo, de dar a conocer y capacitar a los Coordinadores y usuarios del SIIF Nación sobre los procedimientos y trámites administrativos para el manejo del ciclo de vida del certificado digital.

13. La entidad de certificación digital abierta deberá disponer de un contacto directo de soporte de la entidad certificadora con el soporte del SIIF Nación para resolver casos de soporte que involucren las dos partes.

14. La entidad de certificación abierta y la entidad usuaria deberán acordar lo referente a las garantías a que hace referencia el artículo 9 del Decreto 333 de 2014.

DAVID FERNANDO MORALES DOMINGUEZ
Administrador del SIIF Nación
Viceministerio General de Hacienda

APROBÓ: David Morales
ELABORÓ: Jesús Rodríguez