SISTEMA INTEGRADO DE INFORMACION FINANCIERA SIIF NACION
CIRCULAR EXTERNA No. 006

2.0.0.1

Bogotá D. C., 08 de febrero de 2012

PARA: **COORDINADORES Y DELEGADOS 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 en el año 2005, utilizando certificados digitales de función pública expedidos por Entidades de Certificación abierta, siendo para esa fecha la única Entidad Certificadora abierta Certicamara S.A.

La Administración SIIF Nación implementó a partir de la fecha una nueva versión del aplicativo SIIF Nación, que involucró cambios de funcionalidad y tecnológicos para utilizar certificados digitales de función pública emitidos por entidades certificadoras abiertas autorizadas por la Superintendencia de Industria y Comercio.

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 abiertas de confianza para el SIIF Nación:

1. La entidad Certificadora abierta debe estar autorizada por la Superintendencia de Industria y Comercio para expedir certificados digitales de Función Pública.

2. La entidad Certificadora abierta debe estar autorizada por la Administración SIIF Nación para utilizar sus certificados digitales de función pública en el aplicativo SIIF Nación.

   Dicha autorización se emitirá por la Administración SIIF Nación, previa solicitud del representante legal de la entidad Certificadora 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.

3. Los certificados de función pública a utilizar en el SIIF Nación deben estar almacenados en Token Criptográficos con soporte interfaz PKCS11 y que cumplan mínimo con el estándar FIPS 140-1, 140-2 Nivel 3 de aseguramiento criptográfico.

4. La entidad certificadora debe proporcionar a la Administración SIIF Nación, la lista de los token criptográficos a utilizar para el almacenamiento de los certificados digitales y la información técnica para el enrolamiento del token criptográfico en al aplicativo SIIF Nación. Una vez la Administración SIIF Nación informe que dichos token han sido enrolados, podrán ser utilizados en el aplicativo SIIF Nación.

   Para el enrolamiento del token se requiere:

   Librería: ejemplo library=C:\Windows\System32\dkck201.dll
   Nombre: ejemplo name=Alis_Provider

   Estos datos de ejemplo, corresponden a un token Ikey2032.

5. La entidad certificadora debe proveer a sus suscriptores los controladores o drivers para el token criptográfico en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación.

6. Los certificados digitales a utilizar en el aplicativo SIIF Nación para sus usuarios, son certificados de Función Pública con estándar X.509.V3, según las siguientes características:

   a) Nombre
   b) Correo electrónico
   c) Ciudad
   d) Entidad
   e) Cédula de Ciudadanía
   f) NIT de la entidad usuaria
   g) Área = SIIF NACION
      Es importante anotar que todo certificado digital que se usa con el sistema SIIF Nación debe presentar en el campo OU la siguiente información: SIIF NACION (OU=SIIF NACION)
   h) Título o cargo del usuario.
   i) El certificado digital debe utilizar algoritmo de firma: SHA1RSA

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

   a) Autenticación utilizando un terminador de VPN, Juniper, el cual verifica la información del asunto del certificado descrito en el numeral 5 y la confianza de la autoridad de certificación.
   b) Firmar digitalmente transacciones.
   c) Firmar digitalmente archivos para ser utilizados en cargas masivas en el SIIF Nación.

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

8. La entidad certificadora deberá proveer a la Administración SIIF Nación, para la validación del estado de revocación del certificado, la publicación de la CRL[1] con la siguiente extensión marcada como crítica: “Emitir puntos de distribución”, adicionalmente el SIIF Nación utilizará el método de verificación del estado del certificado llamado OCSP[2], para la cual la autoridad de certificación deberá proveer una URL de acceso a este servicio.

   Cualquier cambio de alguno de estos datos debe ser informado previamente por la entidad certificadora 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 certificadora 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.

10. La entidad certificadora 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 certificadora.

11. La entidad certificadora 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 certificadora.

12. La entidad certificadora deberá notificar al usuario y al coordinador SIIF de la Entidad 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.

[1] CRL - Listas de Revocación de Certificados
[2] OCSP - Online Certificate Status Protocol.

13. La entidad certificadora 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, en el horario de lunes a viernes de 8:00 AM a 6:00 PM.

14. La entidad certificadora y la entidad usuaria deberán acordar lo referente a las garantías a que hace referencia el artículo 8 del Decreto 1747 de 2000.

El contenido de este documento podrá ser tenido en cuenta en los procesos de contratación del servicio por parte de cada entidad usuaria o ser ajustados de acuerdo con sus necesidades.

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

APROBÓ: David Morales
ELABORÓ: Jesús Rodríguez