ANEXO No. 1.

CONDICIONES TÉCNICAS EXIGIDAS

La Jurisdicción Especial para la Paz -JEP requiere Certificados digitales de Función Pública como mecanismo robusto de seguridad tecnológica que proporciona validez probatoria jurídica de acuerdo con la Ley 527 de 1999, y que tiene como su principal objetivo, permitir firmar digitalmente las transacciones del aplicativo SIIF NACION II, bajo las siguientes características:

1. La entidad certificadora abierta debe estar autorizada por el Organismo Nacional de Acreditación de Colombia –ONAC, para expedir Certificados Digitales de Función Pública anexar documento que permita constatarlo.

Se solicita que el oferente entregue con su oferta la acreditación ONAC vigente hasta la terminación del contrato, de acuerdo a lo establecido en el numeral 10 del documento justificativo de la contratación "Plazo del contrato", esto en cumplimiento de la obligación establecida en el artículo 160 del Decreto Ley 527 de 1999 en sus artículos 2 literal d, artículo 29 literal a y artículo 30 modificado por el Decreto Ley 0019 de 2012, artículo 42 del decreto 1471 de 2014, que establece las reglas de acreditación y los criterios específicos de Acreditación para las ECD (en adelante CEA-4, 1-10) tomando para ello como documento de referencia la norma internacional ISO/IEC 17065, así como también los modelos y estándares económicos de infraestructura de llave pública (PKI) aceptados internacionalmente).

2. La entidad certificadora abierta debe garantizar que cumple con la certificación autorizada de la Superintendencia de Industria y Comercio, con el fin de proveer la seguridad tecnológica en entornos electrónicos, cumpliendo el marco legal, las normas y estándares, con experiencia en la prestación de estos servicios. (Circular No. 10 de la Superintendencia de Industria y Comercio – Título IV Promoción y control de normas Técnicas).

3. Los certificados digitales deben ser 100% compatibles con el aplicativo SIIF (Sistema Integrado de Información Financiera) del Ministerio de Hacienda y Crédito Público, para lo cual, el proponente debe anexar la certificación de la Administración SIIF Nación, donde se avale la compatibilidad de los certificados emitidos para el intercambio de información con el aplicativo SIIF Nación y la autorización para utilizar sus certificados digitales de función pública en el aplicativo SIIF Nación.

4. 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 140-2 Nivel 3 de aseguramiento criptográfico.

5. La entidad de certificación abierta debe proveer a la Jurisdicción Especial para la Paz -JEP, los controladores o drivers para el token criptográfico en los sistemas operativos utilizados por la entidad usuaria y el soporte para su instalación.

6. Garantizar que los certificados digitales a utilizar en el aplicativo SIIF Nación por los usuarios de la JEP, son certificados de Función Pública con estándar X.509.V3, de acuerdo con los requisitos exigidos en la ley 527 de 1999 y modificaciones realizadas por el Decreto Ley 19 de 2012, Decreto 1747 de 2000, Decreto 333 de 2014 y al título V, Capítulo 8 de la Circular Única del 19 de julio de 2001 expedida por la Superintendencia de lndustria y Comercio y demás normas vigentes, teniendo en cuenta las siguientes características del certificado digital requeridas 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

Es importante observar que todo certificado digital que se usa con el sistema SIIF Nación debe presentar en el campo OU la siguiente información: SIIF NACIÓN (OU=SIIF NACIÓN)

7. Los certificados digitales de función pública se deberán utilizar en el SIIF Nación para las siguientes actividades:

a) Autenticación utilizando un terminador de VPN, Juniper, 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) 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 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 autoridad de certificación 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 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. Es de advertir, que en caso de que cualquier falla en la actualización o disponibilidad de la CRL ocasiona perjuicios a la entidad por no registrar oportunamente, dicha responsabilidad recae directamente sobre la entidad certificadora abierta.

10. La entidad de certificación 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. Así mismo, cualquier falla en la disponibilidad del servicio OCSP, que no permita realizar los registros oportunamente recae directamente sobre la entidad certificadora abierta.

11. La entidad de certificación abierta deberá disponer de la infraestructura de operación, servicio y soporte a los usuarios de los certificados digitales de la Jurisdicción Especial para la Paz -JEP, durante la vigencia del certificado digital, vía telefónica de 8:00 am. a 6:00 pm., de lunes a viernes; acceso vía electrónica a través de la página web, a los servicios de chat, preguntas y respuestas frecuentes y documentación técnica y soporte a través de correo.

12. La entidad certificadora deberá ofrecer las opciones de gestión por parte de la JEP, en cuanto a conocer información relacionada con los certificados, tales como fecha de emisión y fecha de caducidad.

13. La entidad certificadora deberá disponer de un contacto directo de soporte que mantenga comunicación con el soporte del SIIF Nación para resolver casos que involucren las dos partes, el cual deberá estar disponible en horario laboral.

14. Emisión y entrega de Certificados Digitales en dispositivos criptográficos (Tokens) que contenga: Token-Sobreflex con clave, CD de instalación, manual de usuario y manual de software; la caja donde están los dispositivos criptográficos (tokens) y el sobreflex con clave debe ir con sello de seguridad, que permita establecer que no han sido manipulados y las características técnicas y de seguridad de los certificados deben ser de tecnología de punta.

15. La entidad de Certificación Digital Abierta, debe hacer entrega del Certificado de Firma Digital Función Pública en las instalaciones de la Jurisdicción Especial para la Paz-JEP. En caso de que esta entrega se efectúe a través de un operador, éste debe estar certificado mínimo con la norma ISO 9001 (anexar certificación) y se debe indicar a través de correo electrónico al Coordinador SIIF de la JEP el operador logístico con el cual se enviará el Certificado y la guía con la cual fue enviado.

16. La entrega del Certificado de Firma Digital Función Pública al suscriptor deberá ser en un término de dos días una vez emitido.

17. Entregar el certificado digital directamente al suscriptor, previa verificación de su identidad, de forma personal e intransferible. En casos excepcionales, es posible efectuar la entrega del certificado digital a un tercero que actúe como apoderado del suscriptor.

18. Emitir veintidós (22) cupos de Certificados Digitales, los cuales serán utilizados por los usuarios en la operación SIIF.

19. Garantizar la confidencialidad y privacidad por medio de la inscripción de los datos en la transmisión y controlando el intercambio de llaves criptográficas sobre líneas de comunicación inseguras, asegurando que solo el receptor de la información puede acceder a los datos.

20. Garantizar con la firma digital que la información no ha sido manipulada o alterada.

21. Almacenar en cada uno de los dispositivos criptográficos, el certificado digital Token SafeNet IKEY 1000, cuando el supervisor del contrato lo solicite.

22. La entidad de certificación abierta deberá notificar al usuario y al coordinador SIIF de la Jurisdicción Especial para la Paz -JEP por lo menos con un (1) mes de antelación la fecha de vencimiento del certificado digital, así mismo ofrecer al coordinador SIIF Nación

de la JEP, las herramientas para la gestión (Fechas de emisión, fechas de caducidad, cupo utilizado) para una oportuna gestión por parte de los usuarios de los certificados digitales. Así mismo, dará a conocer y capacitar a los usuarios del SIIF Nación sobre los procedimientos y trámites administrativos para el manejo del ciclo de vida del certificado digital.

23. La entidad certificadora deberá garantizar la disponibilidad del servicio, siendo su responsabilidad que sea oportuno y que esté disponible para su consulta durante los 7x24x365.

Nota: Para verificar los numerales 1 y 3, el proponente debe anexar las certificaciones de la ONAC que los autorice para expedir certificados digitales de función pública y del Ministerio de Hacienda, donde se avale la compatibilidad de los certificados emitidos para el intercambio de información con el aplicativo SIIF y la autorización para el uso de sus certificados digitales.