Señores
Proveedores
Ciudad

Referencia: Solicitud de cotización

La UNIDAD DE PLANIFICACIÓN DE TIERRAS RURALES, ADECUACIÓN DE TIERRAS Y USOS AGROPECUARIOS, UPRA, a través de la Secretaría General, requiere adelantar el análisis del sector que tiene como finalidad conocer los aspectos técnicos y económicos del servicio y bienes requeridos por la entidad.

Nota 1: Los interesados en participar en el evento de cotización deberán diligenciar el valor en la plataforma SECOP, incluyendo valor del IVA.

Nota 2: Los interesados cuando lo estimen necesario podrán enviar adicionalmente una propuesta detallada de las características técnicas de los bienes ofertados.

1.1. Objeto del Contrato

FUN_023 Adquisición de certificados digitales de la función pública para ser utilizados por los usuarios del sistema SIIF Nación de la UPRA.

1.2. ESPECIFICACIONES TÉCNICAS REQUERIDAS

ESPECIFICACION	CANTIDAD
Certificados Digitales de **Función Pública** Acreditado AATL-SIIF Nación	11 (once)

CONDICIONES TÉCNICAS MÍNIMAS	
Token de firma digital	
Acreditación de certificados digitales	Los certificados de firma digital deberán ser generados o expedidos a través de una entidad certificada ante por el Organismo Nacional de Acreditación de Colombia (ONAC)
Tipo de Firmante	-Función pública Perteneciente a empresa. Profesional titulado.
Características de los servicios	**Integridad:** En cualquier momento posterior a la firma se podrá demostrar que el documento es el original que se firmó o fue alterado o modificado. **Autenticidad:** Al firmarse directamente por una persona que porta un certificado digital, se puede determinar que el documento es auténtico. **No Repudio:** El firmante del documento no puede repudiar la firma del documento, debido a que es el único custodio del certificado digital o es el único que tiene acceso a él.

Longitud de la llave	2048_bit RSA (software)
Estándar	Almacén de certificados digitales bajo estándar X.509
Algoritmo	Hashing SHA256
vigencia	Mínimo 2 años desde el momento de la activación de cada token
Uso	Firma Digital, No repudio, Cifrado de información. Certificados de función pública puedan ser utilizados en el aplicativo SIIF Nación. Aplicaciones propias de la entidad: Gestor Documental, Aplicativo Contratos.

El par de llaves debe ser generado y almacenado en un dispositivo criptográfico seguro (Token o HSM)

- ✓ La reposición no debe generar costo adicional de acuerdo con las siguientes causales: Retiro, cambio de cargo, daño físico no atribuible al suscriptor, cambio de clave por bloqueo.
- ✓ Reposición del cupo máximo faltando 60 días de su fecha final de caducidad.
- ✓ Reposición del 85% de los cupos adquiridos.
- ✓ Informar el valor de reposición por perdida, sin que esta requiera un cupo nuevo
- ✓ La vigencia del certificado debe iniciar una vez este sea activado.
- ✓ La vigencia de los certificados debe incluir el servicio de soporte técnico y mantenimiento

ESPECIFICACIONES TECNICAS

1. Este servicio de firma digital debe garantizar la connotación de función pública.
2. Este servicio de firma digital acreditada puede ser usado en el Sistema Integrado de Información Financiera SIIF Nación.
3. La entidad de certificación digital informará el procedimiento para la utilización de los certificados digitales para la firma de los documentos.
4. Los certificados deben cumplir con los requisitos exigidos en la normatividad vigente y las demás normas que los complementen o modifiquen.
5. La entidad de certificación digital entregará la documentación técnica y legal correspondiente a los servicios contratados.
6. Los tokens pueden ser utilizados en PC y portátil.
7. La entidad de certificación digital debe garantizar que el servicio es compatible con el sistema operativo Windows 11 y superiores y IOS (MAC) en la versión soportada y liberada por el fabricante. Para el sistema operativo IOS (MAC) el contratista debe realizar las configuraciones que se requieran para la prestación del servicio.
8. La entidad de certificación digital debe suministrar los drivers necesarios para la configuración y uso del sistema operativo Windows 11 y superior, si aplica y de igual manera para los IOS (MAC). En caso de liberarse nuevas versiones de sistema operativo de estos fabricantes, la entidad de certificación digital cuenta con un periodo de transición de máximo 6 meses posteriores a la fecha de lanzamiento de la nueva versión del sistema operativo, para realizar las configuraciones y parametrizaciones necesarias que garanticen la compatibilidad de los certificados de firma con las nuevas versiones de Sistema Operativo.
9. La entidad de certificación digital debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards) vigente y apropiado para la emisión y administración de los certificados de seguridad.
10. El servicio contempla el apoyo técnico y funcional en la implementación del certificado de firma hasta su entrada en operación. Se deben llevar a cabo diferentes pruebas de escrito que permitan validar la correcta funcionalidad del certificado de firma entregado.
11. 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 y debe allegar la acreditación emitida por ONAC.

12. La entidad de certificación digital debe ser miembro de la lista de confianza de Adobe – Adobe Approved Trust List directamente o a través de una de las entidades emisoras de certificados (CA) que hace parte de la lista. En todo caso, la entidad de certificación digital debe garantizar que con los certificados de firma adquiridos por la UPRA acreditados por la ONAC se puede llevar a cabo la validación de ser parte de la lista de confianza.
13. Se debe entregar el certificado emitido por Adobe o enlace de consulta donde se evidencia que la entidad de certificación digital hace parte de la lista de confianza de Adobe - Adobe Approved Trust List.
14. 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 estas especificaciones técnicas y adjuntando los respectivos documentos soporte, una vez realizadas las pruebas técnicas de funcionamiento de los certificados digitales con el aplicativo SIIF Nación. La entidad de certificación digital debe presentar el certificado emitido por la Administración de SIIF Nación del Ministerio de Hacienda que lo acredita como tal.
15. 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.
16. La entidad de certificación digital abierta deberá disponer de la infraestructura de operación, servicio y soporte a sus usuarios, según los siguientes acuerdos de niveles de servicio:

Soporte:

I. La entidad de certificación digital debe brindar el soporte técnico para la implementación, operación y aplicación del certificado de firma durante la vigencia del certificado.
II. La entidad de certificación digital debe disponer de mesa de servicio para atender incidentes y requerimientos a través de canales de atención definidos.
III. La entidad de certificación digital deberá dar solución a los incidentes reportados por la UPRA de acuerdo con la prioridad de los incidentes que se puedan presentar y resolver en los tiempos indicados a continuación, so pena de aplicar el posible incumplimiento.

Prioridad 1: Perdida total del servicio o falla crítica. Efectividad de resolución <= 4 horas hábiles
Prioridad 2: Perdida parcial del servicio o falla no crítica. Efectividad de resolución <= 8 horas hábiles 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.

17. 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.

18. La entidad de certificación digital abierta deberá presentar la garantía que constituyó para el cumplimiento de lo establecido en el artículo 9 del Decreto 333 de 2014.

El Secretario General de la UPRA, expresa su sincero agradecimiento a todos los interesados por la valiosa información suministrada en el marco del presente estudio de mercado. La colaboración recibida constituye un aporte fundamental para el análisis y la toma de decisiones, fortaleciendo la transparencia y la calidad del proceso.