ANEXO 6

Capacidad Técnica

ANDE	Departamento de Sistemas Informáticos División de Tecnología y Desarrollo Informático Dirección de Telemática PLANILLA DE VERIFICACION DE CAPACIDAD TECNICA	Hoja: 1/5

Referencia: Renovación de los Servicios de Soporte y Mantenimiento de Software para la Facturación Electrónica y Módulos de Seguridad HSM (Hardware Security Module) para Gestión de Certificados Digitales.

Especificaciones Técnicas	Características	Mínimo Exigido	El bien/servicio ofertado por la firma PS LINE S.A. cumple con las especificaciones requeridas
Servicios para Facturación Electrónica Se requiere la renovación de los servicios de la solución de software para Facturadores Electrónicos de Paraguay con uso de Certificado Digital en módulo de seguridad HSM.			
1.	Software Facturador Electrónico		
1.1.	La solución debe integrarse al modelo de facturación electrónica del Sistema Integrado de Facturación Electrónica Nacional (SIFEN) de Paraguay, acorde a los requerimientos de la ANDE, cumpliendo con todos los requisitos normativos, técnicos y funcionales que sean requeridos por el SIFEN. La solución deberá cumplir con las especificaciones del Manual Técnico del SIFEN vigente a la fecha de entrega de la misma y con las actualizaciones posteriores, adecuándola a lo establecido en dicho Manual Técnico.	EXIGIDO	CUMPLE
1.2.	Interfaz de servicios web para conectar los sistemas corporativos de la ANDE, que la contratante requiera, con la solución del Oferente.	EXIGIDO	CUMPLE
1.3.	Opción de formulario para carga manual de datos de factura o comprobante electrónico.	EXIGIDO	CUMPLE
1.4.	Generación de Documento Electrónico en formato XML.	EXIGIDO	CUMPLE
1.5.	Firma Digital del Documento Electrónico.	EXIGIDO	CUMPLE
1.6.	Generación, custodia y uso del Certificado Digital en módulo de hardware HSM homologado.	EXIGIDO	CUMPLE
1.7.	Comunicación con SIFEN y envío de Documentos Electrónicos XML firmados digitalmente a la DNIT.	EXIGIDO	CUMPLE
1.8.	Implementación de los mecanismos de comunicación con la DNIT a través de servicios web sincrónicos y asincrónicos.	EXIGIDO	CUMPLE
1.9.	Generación de la representación gráfica de los Documentos Electrónicos, archivos PDF, en el formato KUDE definido por la DNIT.	EXIGIDO	CUMPLE
1.10.	Almacenamiento de datos del proceso.	EXIGIDO	CUMPLE
1.11.	Gestión de envío/recepción de Documentos Tributarios Electrónicos entre emisor/receptor electrónico.	EXIGIDO	CUMPLE
1.12.	Herramienta de configuración del formato de los KUDE.	EXIGIDO	CUMPLE
1.13.	Conector con HSM.	EXIGIDO	CUMPLE
1.14.	Módulo de gestión de usuarios del sistema con un mecanismo de identificación basado como mínimo en usuario y contraseña.	EXIGIDO	CUMPLE
1.15.	Debe permitir la creación de roles y la asignación de los mismos a los usuarios del sistema. Para cada rol el sistema debe permitir configurar a qué opciones puede acceder. Esto debe poder realizarse a nivel de parámetros del sistema.	EXIGIDO	CUMPLE

Referencia: Renovación de los Servicios de Soporte y Mantenimiento de Software para la Facturación Electrónica y Módulos de Seguridad HSM (Hardware Security Module) para Gestión de Certificados Digitales.

1.16. Cómo mínimo debe contar con los siguientes roles: de administración, operación, autorización de firmas y auditoría, pudiendo asignar grupos de usuarios a los mismos.	EXIGIDO	CUMPLE
1.17. La solución debe proveer mecanismos de auditoria para detectar cambios en las configuraciones de la misma.	EXIGIDO	CUMPLE
1.18. La solución debe proveer mecanismos de registro y consulta de todas las operaciones que realiza a través de la generación de logs/registros.	EXIGIDO	CUMPLE
1.19. Debe permitir firmar los comprobantes utilizando certificados digitales de los Prestadores de Servicios de Certificación homologados de Paraguay tal como lo indica la normativa técnica del SIFEN y siguiendo las especificaciones normativas del Ministerio de Industria y Comercio.	EXIGIDO	CUMPLE
1.20. Debe soportar Windows Server o Linux de aplicación Java Websphere, JBoss o Wildfly.	EXIGIDO	CUMPLE
1.21. Debe soportar base de datos Microsoft SQL Server u Oracle	EXIGIDO	CUMPLE
1.22. Debe soportar entornos de virtualización. Indicar cuales.	EXIGIDO	CUMPLE
1.23. Deberán indicarse los mecanismos de integración para el consumo de los servicios de la solución desde los sistemas de facturación.	EXIGIDO	CUMPLE
1.24. La solución implementada debe permitir procesar cien mil facturas electrónicas (generación de XML y KUDE) en un plazo de 2 horas. El oferente deberá indicar los requerimientos de hardware que la contratista debe disponibilizar para cumplir con este plazo.	EXIGIDO	CUMPLE
1.25. La versión de la solución a implementarse deber ser la última estable Ajustes y actualizaciones de versiones, a requerimiento de la Contratante y la DNIT, deberán ser cubiertas durante la vigencia del Contrato.	EXIGIDO	CUMPLE
1.26. La última versión estable debe ser la versión de la solución tecnológica integral a implementarse.	EXIGIDO	CUMPLE
2. Certificado Digital para Facturador Electrónico		
2.1 La oferente deberá proveer un certificado digital, emitido por un Prestador de Servicios de Certificación Autorizado de Paraguay, y con las características requeridas de conformidad o a la normativa técnica vigente del SIFEN y las especificaciones normativas del Ministerio de Industria y Comercio.	EXIGIDO	CUMPLE
2.2. El certificado digital debe cumplir con los siguientes estándares	EXIGIDO	CUMPLE
2.2.1 ITU-T X.509 V.3 Information technology Open systems interconnection TheDirectory: Public-key and attribute certificate frameworks	EXIGIDO	CUMPLE
2.2.2. RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.	EXIGIDO	CUMPLE
2.2.3. RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile	EXIGIDO	CUMPLE
2.2.4. ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".	EXIGIDO	CUMPLE
2.2.5. RFC – 3279 " Internet X.509 Public Key Infrastructure Algorithm Identifier''	EXIGIDO	CUMPLE

Referencia: Renovación de los Servicios de Soporte y Mantenimiento de Software para la Facturación Electrónica y Módulos de Seguridad HSM (Hardware Security Module) para Gestión de Certificados Digitales.

2.3. Los certificados deben ser emitidos por un prestador de servicios de certificación habilitado por el Ministerio de Industria y Comercio, y subordinado a la autoridad de Certificación Raíz del Paraguay.	EXIGIDO	CUMPLE
2.4. La estructura básica del certificado debe estar en conformidad a la norma que rige la materia y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias, conforme a la norma ITU X.509 o ISO/IEC 9594-8	EXIGIDO	CUMPLE
2.5. El certificado digital debe ser válido para firmar facturas electrónicas y cumplir con los requerimientos técnicos exigidos por la Dirección Nacional de Ingresos Tributarios.	EXIGIDO	CUMPLE
2.6. Estructura básica del certificado digital	EXIGIDO	CUMPLE
2.6.1. Versión V3	EXIGIDO	CUMPLE
2.6.2. Número de Serie: Código identificador único del certificado dentro del ámbito del PSC.	EXIGIDO	CUMPLE
2.6.3. Algoritmo de Firma: El algoritmo de firma debe ser como mínimo sha256RSA encryption	EXIGIDO	CUMPLE
2.6.4. Algoritmo hash de firma: sha256	EXIGIDO	CUMPLE
2.6.5. Emisor: Identificación del Prestador de Servicios de Certificación (PSC), con indicación de su Razón Social, RUC, Código de país que se especifica en las directivas obligatorias para la formulación y elaboración de la Política de Certificación y Declaración de prácticas de certificación de los prestadores de servicios de certificación habilitados en la República del Paraguay.	EXIGIDO	CUMPLE
2.6.6. Plazo de vigencia: Fecha de inicio y fecha de Vencimiento	EXIGIDO	CUMPLE
2.6.7. Clave pública del sujeto: Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280 y con un largo de clave de 2048 bits y algoritmo RSA Encryption	EXIGIDO	CUMPLE
2.6.8. Identificador de la Clave del Sujeto: Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública.	EXIGIDO	CUMPLE
2.6.9. Identificador de la clave de la entidad emisora: Debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza.	EXIGIDO	CUMPLE
2.6.10. Uso de la clave: En certificados tipo F1 solamente pueden ser activados los siguientes bits: • NonRepudiation; • digitalSignature; • keyEncipherment.	EXIGIDO	CUMPLE
2.6.11. Uso extendido de la clave: Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage.	EXIGIDO	CUMPLE

Referencia: Renovación de los Servicios de Soporte y Mantenimiento de Software para la Facturación Electrónica y Módulos de Seguridad HSM (Hardware Security Module) para Gestión de Certificados Digitales.

2.6.12. Pólizas de Certificado: Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado.	EXIGIDO	CUMPLE
2.6.13. Restricciones Básicas: En este campo debe ir "TRUE" si el certificado corresponde a una CA o "FALSE" si no corresponde.	EXIGIDO	CUMPLE
2.6.14. CRLDistributionPoints: Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no.	EXIGIDO	CUMPLE
2.6.15. AuthorityInfoAcesss: Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso id-ad-calssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP.	EXIGIDO	CUMPLE
3. HSM		
3.1. Servicio de soporte y mantenimiento de dispositivos criptográficos para las firmas de documentos electrónicos, con módulos para generar y almacenar claves con los niveles de seguridad y autenticación, para protección de las claves, datos y entorno, de acuerdo a estándares.	EXIGIDO	CUMPLE
3.1. El HSM deberá cumplir con lo siguiente:		CUMPLE
3.2.1. Homologación por la Dirección General de Firma Digital y Comercio Exterior para la firma digital.	EXIGIDO	CUMPLE
3.2.2. Homologación por el Ministerio de Industria y Comercio.	EXIGIDO	CUMPLE
3.2.3. Estándar FIPS-2 Level 3 (NIST).	EXIGIDO	CUMPLE
3.2.4. Certificación CC EAL 4+ Common Criteria	EXIGIDO	CUMPLE
3.2.5. Requisitos eIDAS para SSCD - QSCD	EXIGIDO	CUMPLE
Renovavión con Actualización de servicios		
4. Renovación con actualización de servicios		
4.1. Deberán incluirse ciento ochenta (180) horas de soporte para apoyo a la integración a sistemas corporativos de la Contratante y trasferencia de conocimiento u otras tareas, relacionadas al proyecto, que la Contratante requiera.	EXIGIDO	CUMPLE
5. Documentos Solicitados	EXIGIDO	CUMPLE
5.1. Carta de Distribución del Representante, para el software y los servicios ofertados.	EXIGIDO	CUMPLE
5.2. Carta de Autorización del Fabricante, para el software y servicios ofertados.	EXIGIDO	CUMPLE
5.3 El proveedor deberá presentar certificados o constancias de haber cumplido, de manera satisfactoria, implementaciones	EXIGIDO	CUMPLE

similares.		

Lic. Hugo Mujica
Oficina de Ciberseguridad