ADENDA Nº 7

Asunción, 15 DIC. 2017

Se realiza la ADENDA Nº 7, correspondiente al llamado a Licitación Pública Nacional Nº 08/2017 ***"ADQUISICIÓN DE PLATAFORMA CENTRALIZADA DE SERVICIOS AVANZADOS DE CERTIFICACIÓN DIGITAL PARA LA SUBSECRETARIA DE ESTADO DE TRIBUTACIÓN DEL MINISTERIO DE HACIENDA"*** - (ID Nº 336.276).

A continuación se detalla la siguiente modificación realizada al Pliego de Bases y Condiciones, los demás términos, cláusulas y/o referencias **no mencionadas** en esta Adenda **se mantienen invariables**:

- **ENMIENDA Nº 1:** Se realiza la siguiente enmienda en la Sección III. REQUISITOS REQUERIDOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS, quedando la misma redactada de la siguiente manera:

1- ESPECIFICACIONES TÉCNICAS:

ALCANCE: La Subsecretaría de Estado de Tributación precisa adquirir y poner en funcionamiento una plataforma de servicios avanzados de certificación digital, a fin de incorporar todo el ecosistema de certificación digital en procesos internos del Sistema de Gestión Tributaria Marangatu y en un futuro cercano en los procesos relacionados a la implementación del proyecto de Facturación Electrónica.

REQUERIMIENTOS MÍNIMOS:
El sistema deberá prever los siguientes requerimientos mínimos:

- Solución especializada. Brindar toda la funcionalidad completa necesaria para cubrir todos los tipos de operaciones vinculadas al ecosistema de certificación digital
- Hub de servicios: Establecer una infraestructura horizontal para brindar servicios especializados centralizados a toda la institución, accesible desde los diferentes sistemas.
- Integración. Soportar mecanismos de integración estándares y la expansión de interfaces para integrar de forma simple el consumo de los servicios de la plataforma desde los diferentes sistemas de la SET.
- Seguridad: Proveer un esquema de seguridad robusto con niveles de certificación internacionales, incluyendo FIPS y Common Criteria.
- Formatos estándares. Utilizar los estándares internacionales de certificación avanzada aplicables para los formatos y operaciones de firmas, validación y otras vinculadas a la certificación, con soporte a certificados de los prestadores de servicios de certificación homologados de Paraguay.
- Continuidad y calidad del servicio: Soportar alta disponibilidad y alta performance para servicios a la escala requerida.
- Modularidad: Implantar los servicios necesarios y crecer ordenadamente con módulos funcionales.
- Crecimiento funcional incremental: Activar algunas funcionalidades como primera fase, para luego activar otras nuevas y otras características que la SET vaya necesitando.
- Escalabilidad en rendimiento y disponibilidad: Contar con un diseño escalable para el despliegue de proyectos futuros incrementando capacidad del procesamiento y la tolerancia a fallos.
- Transparencia y auditoría. Incorporar mecanismos que permitan recoger todas las pistas de auditoría de la plataforma.

La plataforma deberá prestar inicialmente los siguientes servicios:

- Conexión con PSC
- Custodia de credencial PKI de Persona Jurídica

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MARCIZ CABALLERO MOREIRA
Dirección de Apoyo y de
Administración y Finanzas

- Autenticación de usuarios
- Verificación de identidades
- Firma de personas físicas
- Firma digital de personas jurídica
- Formato firma pdf PADESormato firma xml XADES
- Validación de firmas

Para ello se requiere la provisión de dos módulos de seguridad por hardware (HSM) que funcionen en clúster de modo a ofrecer un esquema de alta disponibilidad y balanceo de carga. Además, debe estar incluida en la oferta la personalización de todas las interfaces requeridas por los sistemas de la SET para el flujo de los procesos identificados en el ítem 4, incluyéndose también soporte y capacitación al personal técnico.

ESPECIFICACIONES TÉCNICAS MÍNIMAS DE LOS BIENES REQUERIDOS PARA LA PLATAFORMA Y SISTEMA

ITEM 1 - PLATAFORMA DE IDENTIFICACIÓN, AUTENTICACIÓN Y FIRMA	
Características	**Especificaciones**
Factor de forma	La plataforma deberá entregarse en formato appliance virtual.
Alcance	El sistema deberá soportar: - la realización de firma digital con una credencial PKI de la SET basada en certificado digital de Persona Jurídica emitido por un Prestador de Servicios de Certificación reconocido en Paraguay por el MIC (Ministerio de Industria y Comercio). - la realización de firma electrónica con credenciales PKI basadas en certificados digitales a ser provistos por la Convocante.
	Debe aglutinar las funcionalidades de autenticación, inicio de sesión único y federación de identidades, para los usuarios con perfil de firma (con credenciales PKI), proporcionando un conjunto de mecanismos de autenticación basados en el contexto con usuario/contraseña, claves de un solo uso, certificados digitales y soporte de dispositivos móviles.
	La plataforma deberá ser escalable y servirá de base para incorporar funcionalidades de firma remota con autenticación segura a los procesos que la SET requiera.
	En particular para el proyecto enmarcado en el presente llamado se deberán proveer todos los componentes para integrarse con dos procesos que serán indicados y definidos por la SET. Deberá proveerse todo lo necesario para el correcto funcionamiento de los mismos.
Certificación	La plataforma deberá contar con una certificación Common Criteria EAL4+ o superior que debe ser entregada junto con la oferta.
Cantidad de usuarios	Inicialmente la SET prevé 1 usuario para la institución SET como persona jurídica y 500 usuarios que serán utilizados por funcionarios, Jefes, Coordinadores y Directores, que interactúen con los Sistemas, servicios y/o procesos en los cuales se requieran el uso de Firmas.
Mecanismos de Configuración	Debe proveer mecanismos de Firma Remota o Centralizada y Servicios de firma masiva en servidor. Para ello el sistema deberá poder gestionar las credenciales PKI de los usuarios (certificados y claves).

Sofía M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MARIA LIZ CABALLERO MOREIRA Directora Interina
Dirección de Apoyo y de
Administración y Finanzas

	La Plataforma de Firma ofrecerá mecanismos de configuración a través de plantillas específicas que permitan determinar la información a devolver a las aplicaciones sobre los certificados y firmas gestionadas.
	La plataforma deberá poder ser configurada mediante políticas específicas que permitan determinar:
	· El mecanismo de autenticación requerido a los usuarios para poder firmar.
	· Los formatos de firma aplicables a un tipo de documento/transacción en función del perfil del usuario o la aplicación demandante.
	· Los certificados y claves a utilizar en un proceso de firma en función de políticas.
Funcionalidad general de firma remota, identificación y autenticación	La plataforma de firma deberá tener mecanismos para interactuar con:
	· Procedimientos de aprovisionamiento de credenciales PKI.
	· Servicios de validación y listas de revocación para validar el estado de los certificados empleados en los procesos de generación y verificación de firmas.
	· Servicios opcionales de Sellado de Tiempo, garantizando que la plataforma pueda soportar la incorporación opcional de sellos de tiempo en las firmas.
	· Dispositivos de hardware de creación de firmas a nivel cliente y servidor.
	Mínimamente se deberán soportar las siguientes interfaces:
	Soportar conectores con CA, RA y VA de PKI, incluyendo Servicios de descarga y cache de CRLs, y TSA.
	Protocolo OCSP de IETF
	Servicios web de autenticación y firma local y remota;
	Interfaces estándar soportadas para dispositivos seguros de creación de firmas. Mínimamente PKCS#11.
	Las credenciales PKI de usuarios gestionados por la plataforma deberán ser albergadas en los HSMs provistos en el ámbito de estas especificaciones técnicas.
	El sistema de gestión de credenciales proporcionado para el proceso de firma remota o centralizada, deberá además garantizar que las credenciales PKI de cada usuario (claves y certificados) quedan bajo el control exclusivo del usuario.
	Debe proveer servicios web para la validación, verificación y actualización de firmas a formatos longevos.
	Debe actuar como un proveedor de Identidad, autenticación y firma frente a múltiples aplicaciones y dispositivos (Servidores, PCs, Tablets, etc.)
	Debe permitir modelar los flujos de identidad y autenticación, solicitando uno o varios factores de autenticación de forma explícita o cuando se supera un umbral de riesgo.
	Debe permitir establecer políticas de Gestión de Riesgo en función del contexto en el que se produce la identificación y autenticación de un usuario.
	Debe permitir la clasificación de los Mecanismos de Autenticación en función de Niveles de Aseguramiento, tal como definen las normas NIST 800-63 o ITU-T X.1254, o similares.
	Debe permitir medidas de contexto que permitan realizar un proceso de elevación del nivel de aseguramiento en función del análisis del contexto del usuario.
	Deberá soportar el establecimiento de procesos de Single SignOn y Federación de Identidad.
	La plataforma soportará la Integración con Directorios externos. Mínimamente LDAP y/o Active Directory.

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas

CABALLERO MOREIRA, Directora Interina
Dirección de Apoyo y de Administración y Finanzas

	La solución deberá soportar múltiples mecanismos de autenticación de usuarios, al menos:
	- Usuario/password
	- OTP por SMS y/o Correo Electrónico.
	- Certificados
	- Redes Sociales: Facebook, LinkedIn, Twitter, etc.
	- Autenticación mediante dispositivos móviles
	La solución debe incluir una aplicación móvil para instalar en dispositivos smartphones o tabletas basadas en sistemas operativos iOS y/o Android, que sirva para i) autenticación; ii) confirmación de transacciones; iii) autorización de firma y firma de documentos; y su integración con las aplicaciones que serán definidas por la SET.
	Los usuarios de esta aplicación serán los mismos usuarios que se indican para la PLATAFORMA DE IDENTIFICACIÓN, AUTENTICACIÓN Y FIRMA en el presente pliego.
	En cuanto al mecanismo de aprovisionamiento de dicha aplicación: se solicita la provisión de los servicios web que puedan ser integrados en un portal de usuario de la SET, donde el propio usuario pueda completar el proceso de aprovisionamiento de dicha aplicación.
	Mínimamente se requerirá que se implementen los mecanismos de autenticación, emisión de un código único de registro en formato QR o textual (que respectivamente pueda ser leído o ingresado en la aplicación móvil), validación de credenciales de registro, generación de claves, emisión de identidad en movilidad (basada en certificado digital) y vinculación de la identidad en movilidad con la identidad centralizada del usuario.
	En cuanto al mecanismo de integración con las aplicaciones requeridas, mínimamente se requiere que las aplicaciones puedan consumir los servicios de la aplicación móvil directamente en forma local (para otras apps móviles) y también a través de un Gateway central de integración que debe formar parte de los entregables de este sistema.
	La plataforma debe poder enlazar con cualquier proveedor de identidad (idP) externo en general. En el contexto del presente proyecto no se utilizarán funcionalidades de autenticación con conexiones a proveedores de identidad de terceros, incluyendo otros IdP o redes sociales, pero debe soportar esta funcionalidad para futuros usos.
	La plataforma debe proveer mecanismos de Integración e Interoperabilidad basadas en las siguientes tecnologías:
	- SOAP, REST, HTTP, HTML, JavaScript, JSON
	- OAuth 2.0, OpenIDConnect 1.0 y SAML 2.0
	Arquitectura SOA orientada a servicios con componentes que permitan una fácil integración con los Sistemas de la institución.
	El usuario final programador podrá hacer uso directamente de los servicios para integrar la firma, validación y otras operaciones avanzadas en sus aplicaciones.
	Acceso a servicios a través de:

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MARLENE CABALLERO MOREIRA, Directora Interina
Dirección de Apoyo y de Administración y Finanzas

	· SOAP/WS con estándar Digital Signature Service de OASIS (DSS) como protocolo de acceso a servicios web, valorándose otros mecanismos de integración.
	· Integración de componentes cliente a través de interfaces abiertas definidas en forma documentada, incluyendo ejemplos de integración.
	· Mecanismos de integración de alto nivel que reduzcan el esfuerzo de desarrollo.
	Se debe proveer un mecanismo de integración a nivel cliente que permita utilizar la interfaz PKCS#11 y CSP para que los usuarios registrados en la PLATAFORMA DE IDENTIFICACIÓN, AUTENTICACIÓN Y FIRMA empleen su credencial PKI a través de este estándar en las aplicaciones que serán definidas por la SET
	El Sistema propuesto debe ofrecer un servicio de identidad digital de firma electrónica (proveedor de firma electrónica) integrado en el proveedor de identidad (IdP) siguiendo el modelo arquitectónico y funcional de OAuth2, es decir, el proveedor de firma debe estar integrado como un servidor de recursos (Resource Server o RS), ofreciendo todos sus servicios mediante API(s) basadas en Web.
	La solución deberá ser escalable y contemplar posibilidades de extensiones con features soportados para actuar como plataforma centralizada de firma y operaciones avanzadas con certificados digitales en entornos cliente y servidor.
Firma, verificación y políticas	Será necesario que la solución cumpla con los siguientes estándares:
	• Estándares de firma electrónica
	o PAdES:
	▪ ETSI TS 102 778
	o XAdES, en los siguientes formatos: BES, EPES, T, C X, XL y A. Se deberán soportar los tipos detached, enveloped y enveloping.
	▪ ETSI TS 101 903
	▪ RFC-2634
	• Estándares de Sello de Tiempo
	o RFC-3161
	• La comunicación con la plataforma central se realizará mediante el protocolo DSS (Digital Signature Service Core Protocols, Elements, and Bindings).
	Si bien la solución inicial requiere firma PDF PADES y XML XADES, será necesario que la solución implemente y sea entregada con la funcionalidad incorporada que cumpla con los siguientes estándares:
	• Estándares de firma electrónica
	o CMS:
	▪ RFC-3852
	o XMLDSig:
	▪ RFC-3275
	▪ ETSI W3C XML Signature Syntax and Processing
	o CAdES, en los siguientes formatos: BES, EPES, T, C X, XL y A. Se deberán soportar los tipos attached y detached.
	▪ ETSI TS 101 733
	• La comunicación con la plataforma se realizará mediante el protocolo DSS (Digital Signature Service Core Protocols, Elements, and Bindings).
	• Otros estándares a cumplir:
	o SAML Core 1.1

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MARIA ... MOREIR I. Directora Interina
Dirección de Apoyo y de Administración y Finanzas

o SAML Core 2.0
o SOAP Version 1.1
o SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)
o ETSI W3C XML Key Management Specification
o OCSP. RFC 6960.
La solución debe soportar dispositivos criptográficos hardware seguros cliente (tarjetas o tokens), asegurando la homologación de los diferentes componentes a ser utilizados.
La solución permitirá la generación de firmas a nivel cliente web con una clave privada individual.
La solución ofrecerá la posibilidad de almacenamiento de claves criptográficas en dispositivo criptográfico hardware (HSM)
La solución debe hacer uso de dispositivos criptográficos hardware seguros a nivel servidor o red (HSMs) para firmas centralizadas.
Posibilidad de utilizar servicios avanzados con certificados digitales para procesos de firma centralizada y masiva, ya sea a nivel de persona física y de persona jurídica.
La solución permitirá la generación de firmas centralizadas ofreciendo la posibilidad de realizar un gran número de firmas con una misma clave privada.
La solución proporcionará un listado de todos los códigos de error devueltos por la aplicación en la respuesta de las peticiones que no se puedan tratar correctamente. Se incluirá la descripción del error, así como los posibles motivos que la han provocado, y la solución de este. Es necesario que la herramienta especifique claramente si se trata de un error de cliente (petición incorrectamente construida o con parámetros incongruentes, etc.), o bien de un error de servidor.
Para llevar a cabo la generación centralizada y validación firmas el sistema deberá implementar el protocolo DSS (Digital Signature Standard) de OASIS. La especificación DSS, concretamente su parte core, describe el protocolo de intercambio de mensajes de petición y respuesta, tanto para el escenario de generación como de validación de firmas electrónicas, utilizando tecnología XML.
La implementación del core del protocolo debe permitir la generación centralizada de firmas electrónicas donde el documento que acompañe a la firma puede ser directamente el documento electrónico o su resumen criptográfico.
La implementación del core del protocolo debe permitir la validación centralizada de firmas electrónicas donde el documento que acompañe a la firma puede ser directamente el documento electrónico o su resumen criptográfico.
Posibilidad de generación y verificación de firmas haciendo uso (o referencia) de políticas de firma.
Una política de firma debe permitir la definición de reglas de firma que aplican al signatario.
Sujeto a lo que permita el formato de firma en cuestión, la política deberá permitir especificar: • Si los documentos firmados son externos a la firma (detached), así como si no lo son (attached, o las formas enveloping y enveloped). • Las propiedades firmadas que deben ser provistas por el firmante. Por ejemplo, el certificado del firmante, el identificador de la política de firma, el rol del signatario etc. • Las propiedades no firmadas que deben ser provistas por el firmante. Por ejemplo, sello de tiempo, información de revocación, etc.
Una política de firma deberá permitir la definición de reglas de validación de la

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MARIA LIZ CABALLERO MOREIRA, Directora Interina
Dirección de Apoyo y de Administración y Finanzas

firma. Las reglas de validación deben permitir la definición de las propiedades no firmadas a incluir en la firma, tanto por parte del firmante, como por parte del validador (en caso de que el firmante no las haya incluido).
Las políticas de firma deben soportar el uso de Commitments (compromisos). Debe ser posible definir un conjunto de reglas a aplicar al conjunto de Commitments de la política, así como definir reglas que apliquen sólo a un commitment concreto.
Las políticas de firma deben permitir la definición de reglas de validación del certificado del firmante, en función de la aplicación de restricciones sobre las entidades de certificación de confianza y los paths de validación.
Las políticas de firma deben permitir la definición de requerimientos de uso de CRLs o cualquier otro servicio de consulta on-line sobre el estado de un certificado, en concreto el uso de servicios OCSP.
Las políticas de firma deben soportar el uso de roles. Los roles deben poder ser alegados o certificados.
Las políticas de firma deben permitir la definición de restricciones sobre las autoridades de sello de tiempo aceptadas, en base a su nombre o al path de certificación para autenticación de la entidad de sellado de tiempo.
Las funciones de gestión de políticas deberán poder definirse a través de la consola web de administración cuando son firmas centralizadas, o interactivamente para firmas individuales.
La solución deberá ser capaz de permitir firmar documentos que ya han sido firmados anteriormente, en cualquiera de los formatos requeridos en este pliego, sin perder ningún dato o firma preexistente.
La solución deberá ser capaz de permitir firmas paralelas. Firmas paralelas son firmas independientes de un mismo documento, donde el orden de generación de las firmas no es importante. Cada firma cubre sólo el documento, pero no ninguna de las firmas anteriores.
La solución deberá ser capaz de permitir firmas consecutivas / Cascada. Permite firmar un documento múltiples veces con un orden entre las firmas definido.
Anidadas (Counter Signature). Las firmas anidadas son un caso concreto de las firmas consecutivas. Las firmas anidadas permiten firmar el valor de una firma anterior, de modo que, implícitamente, cubren también los datos originales. En este caso el orden en que se generan las firmas sí es importante.
Se deberá soportar la firma de documentos de 80MB. Especificar si existen restricciones en cuanto al tamaño máximo recomendado de los documentos a firmar.
La solución deberá implementar el uso de plantillas para la especificación de las propiedades de la firma a generar. Es decir, al hacer la petición de firma de documentos PDF, debe poder indicar qué plantilla de firma se debe utilizar para incorporar la apariencia de la firma visible.
La solución debe permitir enviar en la propia petición de creación de firma la información de visualización o apariencia de la firma en documentos PDF. Es decir, que la información de visualización no estructurará únicamente en plantillas, sino que debe poder ser especificada libremente en la petición de firma, en todas sus posibilidades.
En la información de visualización de apariencia para firma PADES, se debería poder indicar, como mínimo, en relación al posicionamiento y visualización de la firma:
Posicionamiento: • 1 ª página / última página / n ° de página. • Coordenadas y tamaño del recuadro de firma.

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

ALDERO MORÍNIGO
Director Interino
Dirección de Apoyo y de
Administración y Finanzas

• Posibilidad de escoger un campo de firma preexistente
Campos a mostrar a la firma: • Imagen a mostrar en la firma. • CommonName del certificado del firmante • Subject del certificado del firmante. • Nombre y apellidos del firmante. • Cargo del firmante. • Información de contacto. • Organización y / o departamento. • País. • Número de serie del certificado. • Localización donde tiene lugar la firma. • Motivo de la firma. • Fecha de la firma. • Texto fijo que puede aparecer (o no) en la firma.
Configuración de la visualización: • Estilo de los textos que aparecen en la firma.
Los campos anteriores tales que su información se visualizará en la firma, deberán poder ir precedidos, cada uno de ellos, de un título o etiqueta descriptiva determinada. Es necesario que la solución permita indicar el contenido de este título.
La solución comprueba la validez del certificado asociado a la clave con la que se ha solicitado la generación de la firma, antes de llevar a cabo la operación de firma. Si el estado del certificado es suspendido, revocado, o caducado, la firma no se llevará a cabo, y se informará del motivo a la respuesta.
La solución proveerá en la respuesta la firma generada. Esta firma se entregará en función del tipo que corresponda. Es decir, que si se trata de un tipo de firma enveloped, la solución incluirá en la respuesta el documento entero con la firma incluida. Si se trata de una firma enveloping o detached, entonces se devolverá la firma.
La solución deberá proveer el listado de códigos de respuesta de generación de firma que devuelve la plataforma.
La solución deberá permitir la carga y parametrización de las entidades de certificación reconocidas por la organización.
La solución deberá permitir definir y configurar diferentes métodos de validación del estado de los certificados, con un orden de prioridad entre ellos. Los métodos mínimos que debe aceptar son CRL y OCSP.
La validación de certificados y firmas deberá permitir, en la petición, la solicitud de valores de atributos de certificados, de forma Opcional para futura implementación. El sistema proveerá la información solicitada en la misma respuesta de validación.
El valor del atributo solicitado obtendrá de la extensión que corresponda según esté definido en la política del certificado. Es decir, en función de la política del certificado, estos datos podrán estar informadas en una extensión específica del certificado, o en una parte de ésta. El sistema debe ser capaz de analizar la información para obtener los datos solicitados.
La solución deberá proveer el listado de códigos de respuesta de validación de firma que devuelve la plataforma.
La solución deberá dar una respuesta sobre la validez global del documento, y proporcionar detalles sobre la validez de cada una de las firmas del documento.
En el caso de un documento con múltiples firmas, cuando la validación de las

MINISTERIO DE HACIENDA
Subsecretaría de Estado de Tributación
Dirección de Apoyo y de Administración y Finanzas
Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

Dirección de Apoyo y de Administración y Finanzas

	firmas dé como resultado que el documento firmado no es válido, la solución permitirá conocer cuál es el problema y en cuál de las firmas ha localizado el problema. Es decir, que para documentos que contengan más de una firma, la solución debe proveer un resultado global de validación de todo el documento, y el resultado específico de validación de cada una de las firmas. Este resultado debe ser suficientemente explícito en relación al estado de validación de cada firma.
	La validación de firmas de documentos PDF deberá ser capaz de detectar los cambios posteriores a la generación de cada una de las firmas del documento, e identificar estos cambios en la respuesta de validación.
	Si los cambios no vulneran ninguna protección inicial del documento, se informará al cliente de que la firma es válida, pero que se han llevado a cabo modificaciones posteriores en el documento. Si alguna de las firmas del documento protegía este (o partes de éste) de manera que las modificaciones vulneran esta protección, se informará al cliente de que la firma es inválida.
	La solución ofrecerá la posibilidad de validación de firmas por lotes, es decir, debe poder enviar en una única petición de validación, múltiples firmas para validar.
	La solución deberá ser plenamente funcional en la gestión de claves, está gestión se deberá hacer con el estándar XKMS (XML Key Management Specification) y deberá satisfacer los siguientes aspectos: • La gestión de las claves no puede requerir un corte de servicio de la solución. • Los procesos a desarrollar deberán ofrecer las garantías de seguridad técnica y jurídica (incluyendo la gestión de evidencias de los actos) que son necesarias para la correcta generación, instalación y activación o desactivación de claves y certificados digitales. • Las funciones de gestión de claves se deberán poder aplicar a través de la consola web de administración proporcionada por la solución. • La solución también ofrecerá todas las funcionalidades de gestión de claves a través de una interfaz de servicio web o por línea de comandos, para que puedan ser invocadas de forma automática y no únicamente desde la consola de administración. • La gestión de claves mediante interfaz de servicio web debe poder ser securizada mediante el protocolo WS-Security.
Control de acceso central	La solución deberá ofrecer los siguientes tipos de control de acceso y de autorización en sus módulos, teniendo en cuenta las particularidades y necesidades de cada uno de ellos: • Control de acceso abierto. • Control de acceso mediante Usuario + Contraseña. • Control de acceso usando Single Sign-On. • Control de acceso con certificado. • Control de acceso mediante el protocolo WS-Security. • Control de autorización con una granularidad muy fina e implementando SAML.
	La solución debe proveer un control de acceso que permita: • La solución deberá permitir crear políticas de acceso. Por ejemplo, definir una política que permita acceder sólo por LDAP, o una que permita acceder con certificado digital, o bien utilizando Single Sign-On, etc. • La solución deberá permitir el uso de contraseña cifrada. • La solución deberá permitir la operativa (entendida tanto en la gestión como en el uso funcional) con autenticación fuerte basada en certificado digital. En el caso de la autenticación con certificado digital, será necesario que la solución

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MOREIRA I. Directora Interina
Dirección de Apoyo y de
Administración y Finanzas

	verifique la validez del certificado en cuestión. • La solución permitirá implementar el control de acceso a partir del valor de determinados atributos del certificado del cliente. • La solución deberá permitir la integración con LDAP (incluyendo Open LDAP) para la autenticación. • En el caso de la autenticación con LDAP se podrán utilizar los atributos, jerarquía y grupos de usuarios obtenidos del mismo para su uso dentro de la solución. • La solución deberá ofrecer la posibilidad de definir políticas de contraseña. • En el caso de las llamadas a servicios web, estas deberán poder securizar a través del protocolo WS-Security (OASIS Web Services Security (WSS)), para garantizar así la seguridad e integridad de la mensajería.
	La solución proporcionará el control de autorizaciones permitiendo gestionar las capacidades funcionales de los usuarios sobre la solución.
	La solución debe permitir la gestión de usuarios, aplicaciones y grupos, por tanto, la solución proporcionada deberá: • Permitir definir y administrar usuarios. • Permitir definir y administrar aplicaciones. • Permitir definir y administrar grupos de usuarios. • Permitir definir y administrar grupos de aplicaciones. • Permitir la asociación de un usuario a un grupo. No debe haber restricción en el número de grupos a los que puede pertenecer un usuario. • Permitir la asociación de una aplicación a un grupo. No debe haber restricción en el número de grupos a los que puede pertenecer una aplicación. • Permitir definir y administrar roles. Los roles deberán ser asignables a usuarios, grupos de usuarios, aplicaciones, y grupos de aplicaciones. • Permitir asociar políticas de firma usuarios, grupos de usuarios, aplicaciones, y grupos de aplicaciones. • Restringir el acceso a las funciones del sistema según el perfil de usuario y / o sus roles, aplicando controles estrictos de administración del sistema. • La solución deberá permitir la creación y gestión de políticas de identificación. Se entiende como política de identificación aquella que define a partir de qué información se identificará a los clientes. • La solución deberá permitir la creación y gestión de políticas de autenticación. Se entiende como política de autenticación aquella que define los mecanismos de autenticación de los clientes • La solución deberá permitir la creación y gestión de políticas de autorización. Se entiende como política de autorización aquella que define los mecanismos de autorización de los clientes.
Alta disponibilidad y distribución de carga	La solución debe ser escalable para soportar alta disponibilidad y poder desplegarse en modo Activo / Pasivo. Se entiende como Activo / Pasivo cuando se dispone de más de un nodo, pero sólo uno de ellos está sirviendo peticiones. Los otros están a la espera, preparados para servir peticiones si el nodo activo cae, por el motivo que sea. Al hacer el cambio de nodo no se puede perder información, es decir, debe ser totalmente transparente para los clientes. Estos nodos no tienen necesariamente que estar físicamente próximos.
	La solución deberá ser escalable para soportar alta disponibilidad y poder desplegarse en modo Activo / Activo. Se entiende por Activo / Activo la situación en la que hay diferentes nodos sirviendo las peticiones de los usuarios. Las peticiones de un cliente las puede usar cualquiera de los nodos, siendo transparente

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

Dirección de Apoyo y de Administración y Finanzas

	al cliente. Estos nodos no tienen por qué estar físicamente próximos. Cuando uno de los nodos cae pasa a estar inactivo y automáticamente es excluido del clúster sin afectar al servicio.
	La solución deberá poder desplegarse en modo Clúster de Múltiples Nodos. Esta es la situación en la que hay múltiples nodos, interconectados entre ellos, que actúan, externamente, como un único nodo.
	La solución deberá permitir su distribución en varios equipos. Hay que indicar qué porcentaje de carga de tráfico de datos interno necesario, en relación al tráfico de datos externo, dependiendo del número de equipos donde se escala la solución.
	La solución deberá soportar una arquitectura distribuida, es decir que, por ejemplo, deberá permitir instalar la solución en diferentes localizaciones, pero administrarla y configurarla desde un único punto.
Integración general	La solución deberá aportar diferentes capacidades de integración con productos de terceros de la solución ofertada, para ello se deberá indicar: • Disponibilidad de herramientas de integración con aplicaciones, ej.: API Java propio, carpetas de filesystem, gateways de integración, etc. • Integración con directorios LDAP (mínimamente Open LDAP), indicar cuales están homologados. • Integración con BBDD, indicar cuales están homologados. • Integración con HSM, indicar cuales están homologados. • Integración con Splunk. • Integración con sistemas de monitorización SNMP, indicar cuales. • Otros sistemas, indicar cuales.
Administración	La solución deberá incorporar herramientas de administración propias, la más importante de las cuales será una consola web de administración.
	Al menos el 90% de las tareas de mantenimiento de la solución, y en especial la configuración de las prestaciones funcionales, deberá poder realizarse a través de la consola web de administración de la solución.
	La consola web de administración de la solución deberá ser intuitiva, amigable, ergonómica y sobre todo fácil de utilizar, a la vez que operativa y completa.
	La consola web de administración de la solución deberá ser accesible a través de Internet, que permita llevar a cabo una administración remota.
	Hay que especificar en qué casos la aplicación de nuevas configuraciones a la solución requerirá un corte en el servicio.
	La consola tendrá que estar disponible en español.
Backup, recuperación y monitorización	Será necesario que la solución ofrezca un sistema que permita realizar una copia de seguridad de la configuración de la misma.
	La solución deberá ofrecer una solución para restaurar la configuración almacenada en una copia de seguridad, sin que afecte a su integridad.
	La solución se tendrá que integrar fácilmente con herramientas de monitorización. Mínimamente deberá ser compatible con AccelOps y Nagios. Indicar mecanismos de integración.
	La solución deberá permitir que, a través de las herramientas de monitorización, sea posible controlar, al menos, el rendimiento de los procesadores, el estado de la memoria RAM, la capacidad total y ocupada de los espacios de almacenamiento, etc.
Instalación	La instalación se realizará en el servidor que la Convocante pondrá a disposición para el proyecto.
Capacidad y Experiencia	El oferente deberá contar con certificación ISO 9001 o similar en la venta, instalación y posterior soporte post-venta en equipos de TICs. Esto permitirá

MINISTERIO DE HACIENDA – Subsecretaría de Estado de Tributación – Dirección de Apoyo y de Administración y Finanzas – Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

DIRECCIÓN [illegible] Directora Interina
Apoyo y de
Administración y Finanzas

	garantizar a la convocante que el cliente cumple con estándares internacionales de calidad en implementación de este tipo de soluciones. El oferente deberá contar con al menos 1 experiencia previa en la implementación de sistemas de certificación digital similares a los requeridos en el presente pliego. Se deberá demostrar por medio de copias de contratos o facturas.
Garantía y soporte	Soporte y actualizaciones por 24 meses como mínimo.
Autorización del Fabricante	Se deberá incluir una autorización del fabricante para presentar oferta

ITEM 2 - DISPOSITIVOS DE SEGURIDAD POR HARDWARE	
Características	**Especificaciones**
Cantidad	1 (un) clúster de 2 (dos) dispositivos criptográficos HSM (Hardware Security Modules o Dispositivos de seguridad por Hardware)
Funcionalidad general	Funciones seguras de criptografía, de administración de los dispositivos HSM y de gestión del material criptográfico. Deben implementarse procedimientos de contingencia y recuperación de los dispositivos HSM
	Deben implementarse para el proyecto todas las funciones necesarias de generación de claves asimétricas, activación de claves privadas, y creación segura de firmas. El tratamiento de la clave pública y privada vinculada con el certificado de Firma Digital solicitado por la Convocante se realizará acorde a lo que se establezca en la normativa y en coordinación con el PSC emisor.
Certificación	Deberá contar con certificación FIPS 2 nivel 3. Deberá contar con certificación CC EAL 4+. Deberá estar homologado por el Ministerio de Industria y Comercio para ser utilizado como dispositivo criptográfico de firma digital.
Características	Los HSMs deberán soportar funcionalidad en clúster para configuración en alta disponibilidad, de modo a que un usuario pueda autenticarse con su único conjunto de credenciales frente al clúster de dispositivos.
	Deben soportar generación de claves asimétricas y uso de la clave privada en forma interna.
	Se deberá asegurar la custodia con alta disponibilidad de tal forma que las claves solo puedan utilizarse dentro de los HSMs del conjunto.
	Los HSMs deberán soportar funcionamiento standalone (cada HSM funcionando en forma independiente) y clustering (el conjunto de HSMs debe poder operar en Alta Disponibilidad en modo Activo-Activo).
	Se deben incluir todos los componentes necesarios a nivel de hardware y software para incorporar load-balancing automático y configurable de manual para balancear la atención y distribución de solicitudes de servicio y su procesamiento en el clúster de HSMs.
	Deben soportar factores de autenticación multifactor con quórums del tipo "k de n".
	Los HSMs deben soportar al menos los siguientes algoritmos:

Sedra M. Sánchez D.
JEFA INTERINA
DEPTO. DE CONTRATACIONES

MARIA E. CABALLERO MOREIRA, Directora Interina
Dirección de Apoyo y de Administración y Finanzas

	• Simétricos: o AES (128, 192 y 256 bits) o Triple DES (112 y 168 bits) • Asimétricos o RSA (hasta 8192 bits) o Diffie-Hellman o DSA o ECC Suite B • Hashing o SHA-1 y SHA-2 Los HSMs deben entregarse con las librerías de interfaces que soporten: • PKCS#11 • Java (JCE) • Microsoft CAPI y CNG El oferente adjudicado deberá incluir la documentación técnica de todas las funciones disponibles para cada una de las interfaces disponibles y para sus configuraciones, así como los comandos y herramientas de administración y operación. Cada HSM debe ser provisto en para alojar en un rack de 19" de 1U Debe poseer teclado propio y controles con panel integrado en el mismo dispositivo. El acceso a los mismos debe ser posible de proteger con mecanismos genéricos para operaciones básicas del grupo de operación autorizado más factores de autenticación multifactor individuales. Debe poseer redundancia interna para fuente de alimentación con posibilidad de recambio hotswap y de ventilación/refrigeración. Separación de roles de administración y operación. Separación lógica de claves de aplicación Soporte a diagnósticos del tipo Syslog Interfase de línea de commandos e interface gráfica de usuario para administración y operación. Agente de monitorio SNMP: Deben soportar monitoreo del tipo SNMPv3 compatible Generación de logs con almacenamiento interno y servidor de archivos externo. Cada HSM debe disponer de conexión de red a través de al menos dos puertos Ethernet Gigabit que se puedan conectar a segmentos de red diferentes.
Performance	Cada HSM debe soportar al menos 450 tps para largos de clave de 2048 bits. La unidad de tps requerida son firmas por Segundo, y está referida a la performance de firma con RSA para largos de la clave recomendados por el NIST. Es obligatorio indicar cuales son las posibilidades de escalamiento futuro, tanto a nivel individual de cada HSM como del clúster, a efectos de poder soportar la implementación piloto del proyecto de Factura Electrónica.
Cantidad de claves	Almacenamiento protegido de un número ilimitado de claves. Es obligatorio indicar las restricciones para gestión del número de claves soportado y los esquemas de crecimiento.
Garantía y Soporte	Garantía de 24 meses del fabricante, con reposición del equipo en caso falla, en un plazo no mayor de 30 días.

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MINISTERIO DE HACIENDA
Subsecretaría de Estado de Tributación
Dirección de Apoyo y de Administración y Finanzas
Departamento de Contrataciones

MINISTERIO DE HACIENDA
Subsecretaría de Estado de Tributación
Dirección de Apoyo y de Administración y Finanzas
DIRECCIÓN

...RO MORETA, Directora Interina
...n de Apoyo y de
...stración y Finanzas

Autorización del Fabricante	Se deberá presentar una carta de autorización del fabricante para presentar oferta de sus equipos en esta licitación.

ITEM 3 - CERTIFICADOS DIGITALES	
Características	**Especificaciones**
Cantidad	1 certificado Digital de Persona Jurídica para Firma Digital.
Funcionalidad	Los certificados deben corresponder a una subordinada a la Autoridad Raíz de la Infraestructura de Clave Pública de Paraguay, siendo emitidos por un Prestador de Servicios de Certificación homologado en Paraguay por el MIC (Ministerio de Industria y Comercio) y contar con estos perfiles:
	· Todos los certificados emitidos deben corresponder al estándarX.509 versión 3.
	· ITU-T X.509 V.3 Information technology Open systems interconnection
	· The Directory: Public-key and attribute certificate frameworks
	· RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
	· ETSI TS 101 862 V.1.3.3 Qualified Certificates Profile
	·RFC 3739 "Internet X.509 Public Key Infrastructure-Qualified Certificates Profile
	·ISO 3166-1 "Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países".
	·RFC – 3279 '' Internet X.509 Public Key Infrastructure Algorithm Identifier''
	·ITU-T X.509 V.3 Information technology Open systems interconnection
	· El largo de clave de los certificados digitales deberá ser de mínimo 2048bits y estar acorde a las políticas de firma digital definidas por la AC Raíz de Paraguay.
	El certificado digital deberá ser emitido utilizando un dispositivo criptográfico HSM que forma parte de este llamado. La emisión deberá cumplir con la política del PSC bajo la reglamentación del MIC.
	La validez de los certificados digitales deberá ser de 2 (dos) años.
	Se deberán coordinar los procesos y procedimientos de emisión de los certificados digitales.
	El proveedor de los certificados digitales deberá brindar puntos de acceso para CRL y servicios de validación en línea del tipo OCSP para permitir comprobar el estado de los certificados digitales que se adquieran.
Autorización	Autorización del prestador de servicios de certificación, reconocido en Paraguay por el MIC.

ITEM 4 - SERVICIOS DE INSTALACION, PUESTA EN MARCHA, INTEGRACION, GARANTIAS Y SOPORTE	
Características	**Especificaciones**

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

Dirección de Apoyo y de Administración y Finanzas

Cantidad	Global
	Análisis de requerimientos, diseño e implementación y configuración de la plataforma de servicios de certificación, con los mecanismos de autenticación que sean acordados y requeridos por la SET, en la etapa de definiciones de los dos procesos a integrar.
	Configuración de, entre otros:
	· Servicios de firma con formatos avanzados de firma PDF y XML.
	· Uso de claves con los HSMs.
	· Entorno de seguridad, operación y administración del HSM. Debe incluir: Definición de la arquitectura de HSMs y entorno de seguridad, diseño y elección de las opciones de protección de claves, y las opciones de instalación, Configuración de HSMs y entorno de seguridad, e inicialización de los HSM con los roles de administración y operación, y creación de los procedimientos de contingencia. Lo requerido para la correcta implementación inicial del HSM, deberá ser previsto por el oferente. Se debe brindar apoyo a la SET para la definición de los roles de administración y operación.
	· Lo necesario para la implementación inicial deberá ser previsto por el oferente, en particular se requiere que en el proyecto se brinde soporte especializado en todo lo referido a la configuración inicial de la plataforma y a la inicialización de los HSMs.
	· Configuración y soporte para la generación de la solicitud del certificado al PSC. · Configuración y soporte para instalación del certificado que emitirá el PSC.
	· Mecanismos de autenticación con uno y dos factores según el tipo de operación y su ponderación en función de la seguridad y usabilidad requerida.
	· Un proveedor de identidades IDP interno a la plataforma o de la organización.
	·Configuración de los servicios de autenticación y firma de la plataforma y los HSMs, y protección del certificado y clave de firma.
	· Configuración de métodos de firma simple o múltiple encadenada de un mismo documento u operación electrónica.
	· Configuración de apariencias de firma
	· Servicios para verificación firmas de documentos y de datos, y validación de certificados de forma centralizada.
	· Flujos de firma para usuarios internos de la organización.
	· Provisión de un módulo o APIs de integración que brinden servicios a procesos masivos que requieren operaciones criptográficas de firma, verificación y sellado, y que permita automatizar las tareas de definición e implementación de procesos por lotes, para los dos sistemas/procesos que serán definidos por la SET.
	· Un punto único de agregación de datos, auditoria, reporting.
	· Esquema de backups y recuperación
	· Configuración de alta disponibilidad (interno a las plataformas).
Customización de interfaces de integración con la SET	Diseño e implementación de los mecanismos de integración e interfaces para brindar servicios de firma para los procesos de Crédito Tributario y Certificado de Deuda.
	Configuración del esquema de consumo de APIs evaluando los factores que se acuerden para facilitar su integración.
Instalación	La Convocante pondrá a disposición del Oferente adjudicado la infraestructura física adecuada para instalación de las herramientas, así como los servicios de red complementarios (conexión de red, balanceo de carga, servidores, otros).
	Preparación de los appliance virtuales y máquinas virtuales.

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación DIRECCIÓN

Dirección de Apoyo y de Administración y Finanzas

	Instalación de los componentes virtuales en servidores (hardware) disponibles.
	Instalación y configuración de los componentes físicos.
	Carga de las configuraciones e integración con los desarrollos para la SET.
Soporte para integración de las funcionalidades de certificación en los Sistemas de la SET	El Oferente brindara a la SET en el momento que esta lo requiera, todo el soporte necesario para la integración de la plataforma a los dos sistemas/procesos que serán definidos por la SET.
Capacitación	El Oferente adjudicado deberá de presentar un Plan de Capacitación y proveer todos los recursos para el entrenamiento teórico y práctico a (3) tres técnicos de la Subsecretaría de Estado de Tributación como mínimo; en la instalación, configuración y administración de la solución ofertada, la Capacitación deberá incluir mínimamente lo siguiente: Los días necesarios (5 mínimos) de asistencia para integración de la plataforma en módulos que se acordarán en el plan de capacitación, debiendo incluir: • Introducción a la certificación digital. • Visión general de la solución • Arquitectura de la solución • Configuraciones necesarias para brindar diferentes servicios • Operar los equipos realizando tareas de monitoreo, pruebas y ajustes en servicios necesarios para mantener el sistema en condiciones de operación normal. • Mantener el equipamiento en su estado operacional nominal a través de un programa de mantenimiento preventivo y correctivo. • Instrucciones y procedimientos para mantenimientos de emergencia • Capacitación al usuario integrador, mínimamente considerar: o Guía de integración o Ejemplos de uso para integración • Capacitación a Administradores y Operadores • Capacitación para HelpDesk interno de la entidad desde donde se brinda soporte a los usuarios finales. La capacitación deberá ser realizada en las instalaciones de la SET, en caso de ser necesario capacitación en el exterior el oferente correrá con todos los gastos que eso conlleve. Esta capacitación deberá ser realizada durante el período de ejecución del proyecto según cronograma propuesto por el oferente y acordado con la SET, con una duración mínima de 20 hs., para lo cual el Oferente deberá de presentar una Carta Compromiso a través de la cual se compromete a realizar dicha capacitación
Evaluación de Capacidad y Experiencia	El oferente deberá contar con certificación ISO 9001 o similar en la venta, instalación y posterior soporte post-venta en equipos de TICs. Esto permitirá garantizar a la convocante que el cliente cumple con estándares internacionales de calidad en implementación de este tipo de soluciones.
	El oferente deberá contar con al menos 1 (una) experiencia previa en la implementación de sistemas de certificación digital que contemple infraestructuras como las solicitadas en estas especificaciones técnicas. Se deberá demostrar por medio de copias de contratos o facturas.
	La Convocante podrá solicitar una demostración de la plataforma de identificación, autenticación y firma en un entorno de prueba real para validar el nivel de cumplimiento de las funcionalidades solicitadas en el presente pliego. La

MINISTERIO DE HACIENDA
Subsecretaría de Estado de Tributación
Dirección de Apoyo y de Administración y Finanzas
Departamento de Contrataciones

Sandra M. Sánchez D.
JEFA INTERINA
UNIDAD DE CONTRATACIONES

MINISTERIO DE HACIENDA
Subsecretaría de Estado de Tributación
DIRECCIÓN

Dirección de Apoyo y de Administración y Finanzas

	demostración deberá incluir: 1. Presentación técnica de todas las funcionalidades del producto y sus mecanismos de integración. 2. Demostración de la herramienta de configuración y administración del producto. 3. Una maqueta demostrativa, que a modo de referencia deberá incluir como mínimo las siguientes funcionalidades: generación de una identidad PKI en línea y custodia central de la misma, autenticación del titular y autorización de firma mediante mecanismos de 2 factores, proceso de firma remota en formato XADES y PADES utilizando dicha identidad PKI y las APIs o servicios de integración de la plataforma, creación de políticas de validación de firma e integración con los procesos de firma de la demostración. Se permitirá al personal designado por la Convocante, acompañado por técnicos del Oferente, el acceso en modo auditor a la plataforma que se utilice para los fines de esta demostración. Esto deberá realizarse dentro de un plazo máximo de 5 (cinco) días corridos contados desde la solicitud escrita por parte de la Convocante.
Puesta en marcha Servicios de Garantía y soporte	Soporte a las tareas de testing.
	Acompañamiento en la liberación a producción de los procesos/sistemas definidos por la SET.
	Se requiere garantía escrita de dos años emitida por el fabricante de cada uno de los componentes solicitados en estas especificaciones técnicas y su representante en Paraguay con disponibilidad de personal técnico e infraestructura apropiada para el cumplimiento de los niveles de servicio especificados.
	La garantía de funcionamiento aplicará para desperfectos de funcionamiento del producto cuando se producen diferencias entre el funcionamiento originalmente definido y los resultados obtenidos.
	Mesa de ayuda, Soporte y Asistencia local por un período de 24 meses con modalidad 8x5, durante el periodo de vigencia del Contrato.
	Debe incluir soporte del fabricante por este periodo.
	Debe ser realizado por personal capacitado en el producto, el oferente deberá contar con un mínimo de 2 (dos) técnicos especializados por el fabricante en la solución ofertada.
	El servicio debe estar orientado a resolver rápidamente consultas y/o incidentes ya sea en forma presencial (in situ), telefónica, vía correo electrónico, chat.
	El mismo deberá atender en modalidad 8x5 días hábiles horario de 8:00 a 17:00 para evacuar consultas, realizar tareas de diagnóstico, resolver incidentes, realizar trabajos sobre la instalación, con escalamiento de casos al soporte de segundo y tercer nivel, y seguimiento de los mismos hasta su resolución.
	El servicio de instalación contemplará todos los suministros, actividades de montaje, instalación en general, configuración y puesta en funcionamiento de la solución ofertada en el gabinete designado por la Subsecretaría de Estado de Tributación.
	Todos los accesorios requeridos para la instalación de toda la solución deberán ser proveídos por el Oferente
	El Oferente, a través de una constancia emitida por el Fabricante, garantizará por un periodo mínimo de 5 (cinco) años que estará en condiciones de proveer repuestos para los equipos y servicios suministrados.
	El oferente deberá garantizar con una constancia emitida por el fabricante que los equipos son nuevos y de última generación para la familia de equipos ofertados. Los equipos no deben tener fecha de finalización de comercialización publicada.

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MARIA LUZ CABALLERO MOREIRA
Dirección de Apoyo y de Administración y Finanzas

REQUERIMIENTOS ADICIONALES

Conforme los avances que se sucedieren en el Proyecto de Factura Electrónica en la etapa de implementación del Piloto, la SET podrá requerir ampliaciones de servicios de la Plataforma de identificación, autenticación y firma a fin de integrar el Proyecto de Factura Electrónica con la infraestructura adquirida, este requerimiento y su eventual aceptación deberán circunscribirse a las normas de Contrataciones vigentes y de acuerdo a la legislación y plazos establecidos para el efecto.

SEGUIMIENTO Y SUPERVISION

Será competencia de la Coordinación de Sistemas y la Coordinación de Infraestructura de la Dirección de TIC's de la SET según corresponda, las siguientes acciones:

- Designar y priorizar los trabajos a realizar.
- Aprobar o rechazar los trabajos realizados.
- Validar los informes del cumplimiento de los servicios e instalaciones realizadas.

PROPIEDAD INTELECTUAL

Todos los documentos generados por la empresa encargada del servicio serán de propiedad exclusiva de la SET, comprometiéndose a guardar discreción profesional y confidencialidad de todo el trabajo elaborado. La pérdida total o parcial de informaciones, no exime al Contratista de su responsabilidad Civil, Penal, Personal, además de las que surjan de la trasgresión del Artículo 190 de la Ley N° 125/91.

OBLIGACIONES DEL CONTRATISTA

Será de entera responsabilidad del Contratista todos los daños causados a los bienes de la Convocante, provenientes de hechos u omisiones voluntarias o involuntarias, negligencia o inexperiencia de sus empleados, sin cargo alguno para la Convocante.

El contratista asume la plena responsabilidad por el cumplimiento en tiempo y forma de la provisión de los bienes y servicios especificados en la presente Especificaciones Técnicas. Con el fin de deslindar responsabilidades, el oferente deberá informar por escrito, inmediatamente, si existieren razones imponderables que le impedirán cumplir con cualquiera de estos términos de referencia. El oferente deberá arrimar todos los antecedentes necesarios que permitan a la Contratante evidenciar de manera indubitable los preceptos que se deben cumplir para demandar los motivos de fuerza mayor.

El suministro de los bienes y servicios deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en estas Especificaciones Técnicas, pero que pueda inferirse razonablemente que son necesarios para satisfacer lo requerido. Por lo tanto, dichos servicios y/o bienes accesorios o conexos serán suministrados por el Oferente como si hubiesen sido expresamente mencionados.

El OFERENTE ADJUDICADO no podrá aprovecharse de ningún error aparente u omisión que hubiere en las Especificaciones Técnicas. Si se descubriese algún error aparente o discrepancia, deberá informar a LA CONVOCANTE para que lo interprete y dilucide. La decisión de ésta será inapelable.

En todos los casos los precios incluyen los insumos y la mano de obra a más de otros gastos que demanden la instalación de los bienes y servicios adjudicados.

2. CRONOGRAMA Y PLAN DE ENTREGA:

El Oferente deberá de entregar un Cronograma de tareas conforme al Plan de Entrega establecido, en los mismos se especificarán las tareas que serán realizadas en el proyecto de provisión e implementación de la plataforma, así como los servicios conexos y soportes requeridos.

N°	DESCRIPCIÓN	UNID. DE MED.	CANT.	LUGAR DE ENTREGA	FECHA(S) DE ENTREGA
Ítem 1	PLATAFORMA DE IDENTIFICACIÓN, AUTENTICACIÓN Y FIRMA	Unidad		Dirección de TIC-Coordinación de Infraestructura - SET	30 días corridos a la recepción de la Orden Compra/Servicio

MINISTERIO DE HACIENDA Subsecretaría de Estado de Tributación Dirección de Apoyo y de Administración y Finanzas Departamento de Contrataciones

Sonia M. Sánchez D.
JEFA INTERINA
DPTO. DE CONTRATACIONES

MINISTERIO DE HACIENDA DIRECCION

Dirección de Apoyo y de Administración y Finanzas

Ítem 2	DISPOSITIVOS DE SEGURIDAD POR HARDWARE	Unidad	2	Dirección de TIC-Coordinación de Infraestructura - SET	60 días corridos a la recepción de la Orden Compra/Servicio
Ítem 3	CERTIFICADOS DIGITALES	Unidad	1	Dirección de TIC-Coordinación de Infraestructura - SET	90 días hábiles a la recepción de la Orden Compra/Servicio
Ítem 4	SERVICIOS DE INSTALACION, PUESTA EN MARCHA, INTEGRACION, GARANTIAS Y SOPORTE	Global	1	Dirección de TIC-Coordinación de Infraestructura - SET	120 días hábiles posteriores a la recepción de la Orden de Compra/Servicios

Los pagos serán realizados conforme a la siguiente tabla:

N°	DESCRIPCIÓN	UNIDAD DE MED.	CANT.	BIENES Y SERVICIOS
Ítem 1	Entrega de Plataforma de Identificación, Autenticación y Firma	Unidad	1	Con la entrega de la Plataforma de identificación, autenticación y firma
ítem 2	Entrega de Dispositivos de Seguridad por Hardware	Unidad	2	Con la entrega de los Dispositivos de Seguridad por Hardware
Ítem 3	Entrega de Certificados Digitales	Unidad	1	Con la entrega de los Certificados Digitales

Porcentaje

Ítem 4	Servicio de Instalación de la Plataforma de Identificación, Autenticación y Firma	Global	1	30%	Con la instalación de los ítems 1 y 2
	Configuración de la Plataforma y Capacitación	Global	1	20%	Con la conclusión de configuración de la plataforma de certificación digital y la capacitación
	Integración de los 2 procesos (Crédito Tributario y Certificado de Deuda)	Global	1	50%	Con la plena integración de los procesos de Crédito Tributario y Certificado de Deuda, identificados en el ítem 4, indicado como "Customización de Interfaces de Integración con la SET"

Observación: La orden de compra y/o servicio será emitida a más tardar hasta el 31 (treinta y un) de diciembre de 2018. El oferente para solicitar la Póliza de Cumplimiento Contractual deberá considerar este plazo, el plazo máximo Cronograma de Entrega, más un período de 30 (treinta) días calendarios posterior a la finalización de la misma.

Atentamente.

Sonia Sanchez, Jefa Interina
Departamento de Contrataciones

***V°B° María Liz Caballero.*, Directora Interina**
Dirección de Apoyo y de Administración y Finanzas

MARÍA LIZ CABALLERO MOREIRA Directora Interina
Dirección de Apoyo y de
Administración y Finanzas