Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 400082 - Lp1666-21 Servicio de Facturador Electrónico y Adquisición de Módulos de HSM - Hardware Security Module

Consulta 1 - CONSULTA TECNICA SOBRE DISPOSITIVO HSM

Consulta	**Fecha de Consulta**	07-10-2021

Que, en el mencionado llamado, específicamente en el pliego de bases y condiciones, documentaciones Anexas, - Especificaciones Técnicas, se encuentran los siguientes requerimientos:

3.1. El HSM deberá cumplir con lo siguiente:
3.2.1. Homologación por la Dirección General de Firma Digital y Comercio Exterior para la firma digital. EXIGIDO
3.2.2. Homologación por el Ministerio de Industria y Comercio. EXIGIDO
3.2.3. Estándar FIPS-2 Level 3 (NIST). EXIGIDO
3.2.4. Certificación CC EAL 4+ Common Criteria EXIGIDO
3.2.5. Requisitos eIDAS para SSCD – QSCD EXIGIDO

Que, conformes se establece en las políticas de certificación de la Autoridad de Certificación Raíz de Paraguay, emanada del Viceministerio de Comercio, DOC-PKI02, V4.0; a efectos de realizar la homologación de los dispositivos Criptograficos (HSM) en Paraguay, el numeral 6.2.11 -CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO indica: Los módulos criptográficos (HSM) de la CA Raíz y de los PSC deben tener la certificación FIPS 140-2 nivel 3 “Overall”, no precisando otro requisito para que una empresa que quiera constituirse como Prestador de Servicio de Confianza. Por tanto, lo solicitado por la ANDE como requerimiento exigido en los Numerales 3.2.4 y 3.2.5 del cuadro anterior, no corresponden a niveles de seguridad exigidos por ninguna norma paraguaya y por ende concluimos que dicho requerimiento no es válido y no debiera de formar parte del pliego de base y condiciones de este llamado.

Que, para ahondar un poco más sobre estos niveles de seguridad solicitados en la Licictación, pasamos a recordar que la “Certificación CC EAL 4+ Common Criteria”, significa: Criterios Comunes en que los Participantes de este Acuerdo comparten los siguientes objetivos:
1. asegurar que las evaluaciones de los productos y perfiles de protección de tecnología de la información (TI) se realicen con estándares altos y consistentes y se considere que contribuyen significativamente a la confianza en la seguridad de esos productos y perfiles;
2. mejorar la disponibilidad de perfiles de protección y productos de TI evaluados y con seguridad mejorada;
3. eliminar la carga de duplicar evaluaciones de productos de TI y perfiles de protección;
4. Mejorar continuamente la eficiencia y la rentabilidad del proceso de evaluación y certificación / validación * para productos de TI y perfiles de protección.
Es decir, es un documento de buenas prácticas en donde sus miembros acuerdan utilizar estos criterios comunes, es imperioso destacar que entre los miembros de esta comunidad que decidieron adoptar estas prácticas o exigencias no se encuentra aún la AC RAIZ PARAGUAY
Que quiere decir EAL4?. Las EAL son los quiere decir “nivel de garantía de evaluación”, en otras palabras se refiere a los estándares de diseño, desarrollo y buenas practicas todo esto en base a los niveles de seguridad que se busca alcanzar en los distintos dispositivos o productos de alta seguridad como lo son los HSM, pudiendo estos ser desde el nivel 1 al 7.
Qué es el eIDAS exactamente?, El Reglamento sobre identificación electrónica y servicios de confianza, es un reglamento único y estandarizado que se aplica en todos los Estados afiliados a la Unión Europea y que, ofrece un marco jurídico para la aceptación de las identidades y las firmas electrónicas, siendo así este requisito en esta licitación pública nacional carece de propiedad al estar incluido dentro del pliego de base y condiciones, ya que se exige y superpone la aplicabilidad de una norma europea a las normas paraguayas, lo cual es inadmisible ya que la misma ni tan siquiera fue homologada por el gobierno paraguayo.

Que, siendo así la Administación Nacional de Electricidad (ANDE), estaría restringiendo la participación de mas posibles oferentes que tienen la capacidad legal y financiera de proveer lo socilitado en este llamado, con mejores prestaciones que la características.

Es mas, estas especificaciones técnicas, reúnen únicamente los requisitos de la marca SafeLayer Thales, ofertado en el mercado local por la empresa PS line S.A., quien juntamente con CODE100 S.A., se sido consultadas para los precios referenciales, lo cual nos sorprende de sobremanera.

Respuesta	**Fecha de Respuesta**	21-10-2021

Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.

Consulta 2 - Item 1.12 Herramienta de configuración del formato de los KUDE:

Consulta	Fecha de Consulta	08-10-2021
Solicitamos detallar las funcionalidades que debe tener esta herramienta de configuración del formato del KUDE (rediseño online del KuDE o un portal de plantillas pre-definidas).		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 3 - Item 2 Certificado Digital para Facturador Electrónico

Consulta	Fecha de Consulta	08-10-2021
Que cantidad de certificados es requerida?		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 4 - Item 1.20 Debe soportar Windows Server o Linux de aplicación Java Websphere, JBoss o Wildfly:

Consulta	Fecha de Consulta	08-10-2021
Solicitamos aclarar si es requerido que la solución esté desarrollada en Java puesto que en el punto 1.2 mencionan una interfaz de servicio web para conectar el sistema de la ANDE y es independiente a la plataforma desarrollada por el oferente. Favor aclarar si la solución deberá soportar Windows y Linux indistintamente o si soportando una de estas plataformas es suficiente. Se deben utilizar los servidores de aplicación Java Websphere, JBoss o Wildfly o esto es de referencia?		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 5 - CONSULTA EETT HSM SOLICITADO

Consulta	Fecha de Consulta	11-10-2021

Que en el llamado en curso, específicamente en el pliego de bases y condiciones, documentaciones Anexas, - Especificaciones Técnicas, se encuentran los siguientes requerimientos: 3.1. El HSM deberá cumplir con lo siguiente: 3.2.1. Homologación por la Dirección General de Firma Digital y Comercio Exterior para la firma digital. EXIGIDO 3.2.2. Homologación por el Ministerio de Industria y Comercio. EXIGIDO 3.2.3. Estándar FIPS-2 Level 3 (NIST). EXIGIDO 3.2.4. Certificación CC EAL 4+ Common Criteria EXIGIDO 3.2.5. Requisitos eIDAS para SSCD – QSCD EXIGIDO Que, conformes se establece en las políticas de certificación de la Autoridad de Certificación Raíz de Paraguay, emanada del Viceministerio de Comercio, DOC-PKI02, V4.0; a efectos de realizar la homologación de los dispositivos Criptográficos (HSM) en Paraguay, el numeral 6.2.11 -CLASIFICACIÓN DEL MÓDULO CRIPTOGRÁFICO indica: Los módulos criptográficos (HSM) de la CA Raíz y de los PSC deben tener la certificación FIPS 140-2 nivel 3 “Overall”, no precisando otro requisito para que una empresa que quiera constituirse como Prestador de Servicio de Confianza. Por tanto, lo solicitado por la ANDE como requerimiento exigido en los Numerales 3.2.4 y 3.2.5 del cuadro anterior, no corresponden a niveles de seguridad exigidos por ninguna norma PARAGUAYA y por ende dicho requerimiento no es válido y no debiera de formar parte del pliego de base y condiciones de este llamado , DEMÁS ESTA DECIR QUE POR ENDE NO ES TÉCNICAMENTE INDISPENSABLE .
Para aclarar un poco más sobre estos niveles de seguridad solicitados en la Licitación, pasamos a recordar que la “Certificación CC EAL 4+ Common Criteria”, significa: Criterios Comunes en que los Participantes de este Acuerdo comparten los siguientes objetivos: 1. asegurar que las evaluaciones de los productos y perfiles de protección de tecnología de la información (TI) se realicen con estándares altos y consistentes y se considere que contribuyen significativamente a la confianza en la seguridad de esos productos y perfiles; 2. mejorar la disponibilidad de perfiles de protección y productos de TI evaluados y con seguridad mejorada; 3. eliminar la carga de duplicar evaluaciones de productos de TI y perfiles de protección; 4. Mejorar continuamente la eficiencia y la rentabilidad del proceso de evaluación y certificación / validación * para productos de TI y perfiles de protección. Es decir, es un documento de buenas prácticas en donde sus miembros acuerdan utilizar estos criterios comunes, es IMPORTANTE destacar que entre los miembros de esta comunidad que decidieron adoptar estas prácticas o exigencias NO SE ENCUENTRA aún la AC RAIZ PARAGUAY .Que quiere decir EAL4?. Las EAL son los quiere decir “nivel de garantía de evaluación”, en otras palabras se refiere a los estándares de diseño, desarrollo y buenas prácticas todo esto en base a los niveles de seguridad que se busca alcanzar en los distintos dispositivos o productos de alta seguridad como lo son los HSM, pudiendo estos ser desde el nivel 1 al 7. Qué es el eIDAS exactamente?, El Reglamento sobre identificación electrónica y servicios de confianza, es un reglamento único y estandarizado que se aplica en todos los Estados afiliados a la Unión Europea y que, ofrece un marco jurídico para la aceptación de las identidades y las firmas electrónicas, siendo así este requisito en esta licitación pública nacional carece de propiedad al estar incluido dentro del pliego de base y condiciones, ya que se exige y superpone la aplicabilidad de una norma europea a las normas paraguayas, lo cual es inadmisible ya que la misma ni tan siquiera fue homologada por el gobierno paraguayo. Que, siendo así la Administración Nacional de Electricidad (ANDE), estaría restringiendo la participación de más posibles oferentes que tienen la capacidad legal y financiera de proveer lo solicitado en este llamado, con mejores prestaciones que la características. Es más, estas especificaciones técnicas, reúnen únicamente los requisitos de la marca SafeLayer Thales, ofertado en el mercado local por la empresa PS line S.A.
Por todo lo argumentado , solicitamos esos requisitos que no tienen otro objeto que limitar la libre participación sean totalmente eliminados y permitan a potenciales oferentes con mejores ofertas poder participar del llamado en curso.

Respuesta	Fecha de Respuesta	21-10-2021

Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.

Consulta 6 - Item 1.20 Debe soportar Windows Server o Linux de aplicación Java Websphere, JBoss o Wildfly:

Consulta	Fecha de Consulta	11-10-2021

Favor aclarar si es requerido que la solución esté desarrollada en Java puesto que en el punto 1.2 mencionan una interfaz de servicio web para conectar el sistema de la ANDE y esto es independiente a la plataforma desarrollada por el oferente. Aclarar si la solución deberá soportar Windows y Linux indistintamente o si soportando una de estas plataformas es suficiente. ¿Se deben utilizar los servidores de aplicación Java Websphere, JBoss o Wildfly o esto es de referencia?

Respuesta	Fecha de Respuesta	21-10-2021

Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.

Consulta 7 - Item 1.12 Herramienta de configuración del formato de los KUDE:

Consulta	Fecha de Consulta	11-10-2021
Precisamos detalle de las funcionalidades que debe tener esta herramienta de configuración del formato del KUDE (rediseño online del KuDE o un portal de plantillas pre-definidas).Favor aclarar las mismas.		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 8 - Item 2 Certificado Digital para Facturador Electrónico

Consulta	Fecha de Consulta	11-10-2021
¿Aclarar cantidad de certificados es requeridos?		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 9 - HSM

Consulta	Fecha de Consulta	11-10-2021

Atendiendo la primera consulta ingresada de manera virtual en fecha 07/10/21, sobre las especificaciones de los equipos HSM´s indicados en esta licitación, hemos realizado consulta "Técnica a la Dirección General de Firma Digital y Comercio Electrónico", quien nos contesto en la nota SSECS/DGFDyCE N° 0289/2021, expresando en su parte pertinente: .... "Cabe destacar que la normativa vigente a través de la Resolución Ministerial N° 1400/2016 Anexo III Normas de Algoritmos Criptograficos PKI PARAGUAY VS 1.0 DOC PKI-06 establece los siguientes requerimientos.

En el punto 2 APLICABILIDAD DE LOS ALGORITMOS Y PARAMETROS
CRIPTOGRÁFICOS establece los algoritmos y parámetros que deben ser
utilizados obligatoriamente:
Generación de las Claves Asimétricas de Usuarios finales
Normativa PKI Paraguay DOC-PKI-04- ítem 6.1.5
Algoritmo RSA conforme al RFC 5639
Tamaño de clave F1 y C1 RSA 2048
Tamaño de clave F2 y C2 RSA 2048, RSA 4096
Firma de certificados de Usuarios Finales
Normativa PKI Paraguay DOC-PKI-04- ítem 7.1.3
Suite de Firmas sha256WithRSAEncryption
sha512WithRSAEncryption
En el punto 3 Estándares de Hardware establece los estándares requeridos
para los hardwares criptográficos:
Utilización Requisito
obligatorio
Estándares Norma
Módulo
criptográfico de
generación de
claves asimétricas
para usuario final
Homologado por
el MIC
FIPS 140-1 o FIPS
140-2 (para
certificados tipo
F1 o C1). FIPS 140-

2 nivel 2 o nivel 3 (para certificados tipo F2 o C2). DOC-PKI-03 item 6.2.1 DOC-PKI-04 Ítem 6.2.1 Módulo criptográfico para almacenamiento de la clave privada del titular del certificado Homologado por el MIC FIPS 140-1 o FIPS 140-2 (para certificados tipo F1 o C1). FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2). DOC-PKI-04 Parámetro de generación de claves asimétricas Homologado por el MIC FIPS 140-1 o FIPS 140-2 (para certificados tipo DOC- PKI -04 ítem 6.1.6 de usuario final F1 o C1). FIPS 140-2 nivel 2 o nivel 3 (para certificados tipo F2 o C2)
En visto a lo expuesto, esta unidad técnica ratifica que los requerimientos señalados ut supra constituyen los requisitos que deben cumplir los hardware criptográficos utilizados en la PKI Paraguay para generación y almacenamiento de claves asimétricas de usuario final los cuales son considerados por esta unidad técnica al momento de la homologación respectiva....."

Atendiendo todo lo expresado anteriormente y la contestación dada por la Dirección General de Firma Digital y Comercio Electrónico; consultamos puntualmente si la Administración Nacional de Electricidad (ANDE), continuará considerando como exigible los requisitos consignados en el numeral 3 referente a documentaciones Anexas, - Especificaciones Técnicas, específicamente lo relacionado a lo establecido a las certificaciones NO HOMOLOGADAS por el gobierno Paraguayo., numerales 3.2.4 y 3.2.5

Copia de la contestación será entregada vía mesa de entrada física de la ANDE.

Respuesta	**Fecha de Respuesta**	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 10 - Formas y condiciones de Pago

Consulta	Fecha de Consulta	12-10-2021
De acuerdo a las formas y condiciones de pago según el PBC establece el pago mensual para el ITEM 1 Pago mensual por el servicio otorgado durante 36 meses. Favor aclarar si en la planilla de precios, Unidad Medida Global cargamos el precio por el total ofertado o lo que seria el precio mensual multiplicado por la cantidad de meses a facturar?		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 11 - Integración ANDE - sistema facturación electrónica

Consulta	Fecha de Consulta	12-10-2021
¿Qué sistema de facturación cuenta actualmente ANDE? ¿Qué mecanismo de integración tienen planificado utilizar? ¿Quién es el responsable del desarrollo de la interfaz entre el sistema de facturación y el software de factura electrónica? ¿ANDE o proveedor?		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		

Consulta 12 - Condiciones empresa postulante

Consulta	Fecha de Consulta	12-10-2021
¿Es posible presentarse una empresa que tiene más de 19 años operando en Paraguay y que hasta el 31/12/2019 tributaba al IRP al ser una sociedad simple y que solo cuenta con el balance del 2020, ya que por la ley 6380 Art.2 solo hasta el 01/01/2020 estuvo obligada a presentar los mismos? En caso de que sea posible, cómo debe hacer los cálculos de la sección de requisitos financieros del pliego de bases y condiciones sin los datos de 2018 y 2019?		

Respuesta	Fecha de Respuesta	21-10-2021
Sírvase considerar, para la elaboración de sus ofertas, lo establecido en el PBC, EETT y la Adenda No. 1.		