San Lorenzo, 12 de mayo de 2020

ADENDA N° 02

CONTRATACION DIRECTA N° 04/2020

"ADQUISICION DE FIRMAS DIGITALES" - ID N° 376766

Por la que se prorroga la fecha y hora limites conforme a lo establecido en el SICP, para la realización de consultas y entrega de ofertas.

ANEXO C

ESPECIFICACIONES TÉCNICAS DE LOS BIENES O SERVICIOS A SER ADQUIRIDOS

1. Especificaciones Técnicas

DONDE DICE

La empresa a ser contratada deberá prestar servicios de emisión de Certificados Digitales de Personas Físicas y Jurídicas para firma digital y autenticación, calificados en el marco de la PKI Paraguay.

A efecto del servicio y la dinámica de la Institución, se establecerá un procedimiento entre el prestador del servicio de emisión de firmas digitales, y la Sección Informática de la Institución, en el marco del cual se realizará la gestión de los Certificados.
La dinámica de la comunicación para la gestión de los servicios contratados se efectuará a través del correo electrónico desde las cuentas institucionales debidamente identificadas en el marco del procedimiento acordado.
El proveedor deberá contar con servicio móvil de "Agente de Registro" para la gestión de firmas digitales relacionadas a Usuarios que requieren la provisión o reposición inmediata de sus dispositivos de firma, el esquema funcional de este servicio formará igualmente parte del procedimiento acordado entre el Proveedor y la Sección Informática.

El servicio móvil incluirá:

- La presencia del Agente en las Oficinas individualizadas
- La firma digital solicitada
- La instalación de los aplicativos y controladores de los Tokens para la firma digital en los equipos señalados.

OBSERVACION: Los costos del servicio móvil, serán facturados por VISITA del Agente a la institución, independientemente a la cantidad de Firmas Digitales expedidas.

La empresa deberá prestar servicio de Revocación de Certificados digitales expedidos para los Magistrados, Actuarios y Funcionarios Administrativos a solicitud de la Institución, conforme el procedimiento establecido.
Conforme los procedimientos legales establecidos, en lo relativo al ítem 2, la clave privada de los Certificados digitales deberá encontrarse resguardada en dispositivos criptográficos cumpliendo con los niveles de máxima seguridad y exigencias de seguridad de la PKI Paraguay, alineados con las mejores prácticas y los estándares internacionales.
La Sección Informática comunicará al Proveedor los nombres y direcciones de correo institucional de las personas debidamente autorizadas para realizar gestión de Firmas Digitales en nombre de la dependencia. La gestión para la provisión de las Firmas Digitales será efectuada por la Sección Informática utilizando al efecto la comunicación con la Prestadora del Servicio a través del correo electrónico.
En igual sentido el Proveedor establecerá una dirección de correo electrónico en donde recibirá todas las solicitudes de la Circunscripción Judicial del Dpto. Central en el marco del contrato.
La solicitud de emisión de un nuevo certificado de firma digital será enviada en correo electrónico conteniendo claramente el tipo de generación solicitada en base a los Ítems contratados, así como los datos completos del Magistrado o Funcionario para quien se solicita la firma digital, cumpliendo con los requerimientos de información establecidas por el Proveedor para la emisión del certificado.
De igual manera la solicitud de revocación de certificados de firma digital se gestionará por el mecanismo del correo electrónico bajo las mismas condiciones anteriormente indicadas.

Los servicios solicitados son:

ITEM	DESCRIPCION DEL SERVICIO	CANTIDAD	UNDAD DE MEDIDA
1	Provisión de Firma Digital	1	Unidad
2	Provisión de Firma Digital + Dispositivo	1	Unidad
3	Agente de Registro Móvil	1	Unidad

PODER JUDICIAL * CIRCUNSCRIPCIÓN JUDICIAL CENTRAL * UOC

Ing. CASPAR SOSA
Jefe Dpto. de Informática
Circunscripción Judicial Central

QUEDA REDACTADO DE LA SIGUIENTE MANERA:

ESPECIFICACIONES TECNICAS MINIMAS

Certificado Digital

DESCRIPCIÓN	ESPECIFICACIÓN TÉCNICA
1. Emisor	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.
2. Conformes al formato definido por la norma ITU X.509 o ISO/IEC 9594-8.	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
3. Tipo de certificado	Certificado de Persona Física del tipo F2 con Datos Laborales (Firma Digital basado en hardware)
4. Almacenamiento	La clave privada correspondiente al certificado digital debe ser generada en un dispositivo criptográfico (token) que asegure el cumplimiento del estándar FIPS 140 level 3
5. Duración	La validez del certificado digital deberá ser de 24 meses
6. Procedimiento de registro y emisión de certificado y par de claves	Presencial, en el local del Proveedor y/o en el local de la Corte Suprema, cuya duración por proceso no supere 1 (una) hora.
7. Procedimiento de revocación de certificado	Presencial o remoto, el suscriptor debe poder revocar el certificado las 24 horas de los 7 días de la semana.
Estructura del certificado	
Campo Sujeto	
8. País	Código de país es asignado de acuerdo al estándar ISO 3166
9. Organización	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física con datos laborales.
10. Unidad Organizativa	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En este caso se identifica que corresponde a un certificado emitido en módulo hardware.
11. Nombres	Este campo debe contener el/los nombre/s y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apóstrofes si corresponde.

Ing. GASPAR SOSA
Dpto. de Informática
Circunscripción Judicial Cen

12. Número de Serie	Debe contener las siglas CI seguidas del Número de Cédula de Identidad del titular del certificado, según documento de identificación.
13. Nombres	Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apóstrofes si corresponde.
14. Apellidos	Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apóstrofes si corresponde.
Campo Nombre Alternativo del Sujeto	
Rfc822Name	Email del titular del certificado.
15. Nombre de la Empresa	Nombre de la organización en el que presta servicio el titular del certificado.
16. Registro Único de Contribuyente	RUC más Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado.
Campos relevantes	
17. Versión	V3
18. Número de Serie	Código identificador único del certificado dentro del ámbito del PSC
19. Algoritmo de Firma	El algoritmo de firma debe ser como mínimo sha256RSA encryption
20. Algoritmo hash de firma	sha256
21. 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.
22. Plazo de vigencia	Fecha de inicio y fecha de vencimiento
23. 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 o 4096 bits y algoritmo RSA Encryption
24. 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. No es crítico.
25. 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. No es crítico.

Ing. GASPAR SOSA
Jefe Dto. de Informática
Circunscripción Judicial Central

26. Uso de la clave	En certificados tipo F2 solamente pueden ser activados los siguientes bits: · NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); · digitalSignature; · keyEncipherment Si es crítico
27. Uso extendido de la clave	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage. Si es crítico.
28. Políticas del Certificado	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado. No es crítico.
29. Restricciones Básicas	En este campo debe ir "TRUE" si el certificado corresponde a una CA o "FALSE" si no corresponde.
30. Nombre alternativo del sujeto	Campos no obligatorios. Rfc822Name= [email del titular del certificado]
31. 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. No es crítico.
32. 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. No es crítico.

PODER JUDICIAL * CIRCUNSCRIPCION JUDICIAL CENTRAL * UOC

Ing. CASPAR POSA
Jefe Dto. de Informática
Circunscripción Judicial Central

Token de Seguridad

DESCRIPCIÓN	ESPECIFICACIÓN TÉCNICA
1. Sistemas operativos en los que opera (32 o 64 bits)	Windows XP SP3, Server2003 , Windows Vista, Server2008, Windows 7, Windows Server 2012, Windows 8, Windows 10
	Linux
	MAC OS X
2. Middleware	Microsoft Windows MiniDriver
	Windows middleware for Windows CSP
	Direct-called library for PKCS#11 under Windows, Linux and MAC
3. Standards	X.509 v3 Certificate Storage, SSL v3, IPSec, Minimamente ISO 7816 1-4 y opcionalmente ISO 7816 8 9 12, CCID
4. Algoritmos Criptográficos	RSA 2048 bit, como mínimo.
	SHA-1 / SHA-256
5. Longitud de Claves RSA	1024 bits/2048 bits
6. Funciones Criptográficas	Onboardkeypairgeneration
	Onboard digital signature and verification
	Onboard data encryption and decryption
7. APIs Criptográficas	Microsoft Crypto API (CAPI), Cryptography API: Next Generation (CNG)
	Microsoft Smart CardMiniDriver
	PKCS#11
	IPSec/IKE
	PC/SC
8. Procesador	16 bit smart card chip (Common Criteria EAL 5+ certified). El procesador debe estar homologado por el Ministerio de Industria y Comercio (MIC)
9. Espacio de Memoria	Mínimamente: 64KB (EEPROM)
10. Dimensión	Mínimamente: 16,4mm*8,5mm*40,2mm
11. Reescritura de Celdas de Memoria	At least 500,000 write/erase cycles
12. Retención de Datos	Por lo menos 10 años
13. Certificaciones de Seguridad	FIPS 140-2 level 3
14. Interface de Comunicación	USB 1.1 y 2.0 full speed & high speed, Connector type A
15. Interface	ISO 7816
	CCID
16. Consumo de Energía	Less than 250mW. Máximo 5 V.
17. Temperatura de Funcionamiento	0°C ~ 70°C
	(32°F ~ 158°F)

Ing. GASPAR SOSA
Jefa Dto. de Informática
Circunscripción Judicial

18. Temperatura de Almacenamiento	-20°C ~ 85°C (-4°F ~ 185°F)
19. Humedad	0% ~ 100% sin condensación
20. Compatibilidad con especificaciones de la Organización Internacional de Normalización (ISO)	Compatible con las especificaciones 1 a 4 de la Norma ISO/IEC 7816

Servicio de RA Móvil

DESCRIPCIÓN	ESPECIFICACIÓN TÉCNICA
1. RA MOVIL	El proveedor deberá contar con servicio móvil de "Agente de Registro" para la gestión de firmas digitales relacionadas a Usuarios que requieren la provisión o reposición inmediata de sus dispositivos de firma. El servicio móvil incluirá: • La presencia del Agente en las Oficinas individualizadas. • La firma digital solicitada. • La instalación de los aplicativos y controladores de los Tokens para la firma digital en los equipos señalados. OBSERVACIÓN: Los costos del servicio móvil, serán facturados por VISITA del Agente a la institución, independientemente a la cantidad de Firmas Digitales expedidas

Los servicios solicitados son:

ITEM	DESCRIPCION DEL SERVICIO	CANTIDAD	UNDAD DE MEDIDA
1	Certificado digital + Token	1	Unidad
2	Certificado digital	1	Unidad
3	Servicio de RA Móvil	1	Unidad

Observacion: Los demas puntos de la Carta de Invitación se mantienen inalterables.

PODER JUDICIAL * CIRCUNSCRIPCIÓN JUDICIAL DEL DPTO. CENTRAL * UOC

LIC. FRANCISCO CACERES
JEFE – UOC
CSJ – Circunscripción Judicial del Dpto. Central

Ing. GASPAR SOSA
Jefe Dto. de Informática
Circunscripción Judicial Central