

CONDICIONES Y ESPECIFICACIONES TECNICAS DE LOS PRODUCTOS OFERTADOS

CONCURSO DE PRECIOS N° 08/2018

Token Criptográfico - Usuario Final:

Dispositivos token usb de almacenamiento electrónico de alta seguridad para infraestructura de llave pública (PKI).

Especificaciones técnicas mínimas:

- Poseer interfaz USB estándar (Universal Serial Bus)
- Cumplir los estándares PKI exigidos por la IFDRA (Infraestructura de Firma Digital de la República Argentina)
- Poseer un mínimo de 32 Kb dedicado al almacenamiento seguro de llaves públicas/privadas y Certificados
- Generación interna (OnBoard) de claves RSA (mínimo 1024 bits)
- Generación interna de claves DES/3DES
- Algoritmos de firma soportados SHA-1 y MD-5
- Poder almacenar Certificados v3 X.509 v3
- No deberá necesitar otro lector adicional aun puerto USB para su funcionamiento
- Deberá soportar como mínimo los sistemas operativos Windows 7, Windows 8, Windows Server 2012, Windows Server 2008, Ubuntu, Debian
- Licenciamiento perpetuo.
- Actualizaciones del software sin cargo.
- Generación de llaves en 10 segundos o menos.
- Firma de llave en menos de 2 segundo
- Algoritmo RSA seguro en firmware, de 1024 bit,
- Generación de clave y firmas en dispositivos
- Deberá poseer dos niveles de acceso. Uno para el usuario final y otro para el administrador, el cual podrá formatear el dispositivo para poder ser reutilizado
- El dispositivo debe poder importar Certificados X.509 y de llaves públicas/privadas
- El dispositivo no puede permitir exportar la clave privada del certificado, ni hacer copias de backup.
- Se deberá proveer una herramienta de formateo de los dispositivos (smartcard usb) para restaurar la configuración de fábrica (Set to Factory) sin comprometer la seguridad y además recuperar el dispositivo (token usb) para retornarlo a producción en el organismo.
- Deberá proveer la opción de bloquear el acceso vía el administrador
- Se deberá proveer un instalador independiente para los drivers de los dispositivos y el mismo no deberá instalar ninguna herramienta de administración (ni para el usuario ni para el administrador)
- Las herramientas de administración deberán permitir importar las siguientes extensiones de certificados: PFX, P12, P7B, CER
- Los dispositivos criptográficos deben tener una identificación única externo para una identificación fehaciente por parte del organismo, para poder administrar los dispositivos y poder inventariar físicamente los mismos.