FOLIO 2

Dispositivo Criptográfico

Dispositivo criptográfico (Token), Certificado FIPS 140-2 con las siguientes características:

Presentación:

- Carcasa de protección compuesta de un material robusto, resistente al agua y firmemente sellado a fin de no permitir el ingreso de líquidos.
- Características de 'tamper-evident'.
- Interfase estándar USB tipo A.
- Debe tener un LED indicador de actividad.

Características Técnicas:

- Tecnología Plug-and-Play para facilitar su utilización con aplicaciones cliente.
- El dispositivo criptográfico Token USB ofertado deberá contar con certificación FIPS 140-2 level 3 (como mínimo) otorgada para el dispositivo en su totalidad (firmware y hardware) Dicha certificación deberá contar con un plazo de validez no menor a 4 (cuatro) años de la fecha de recepción de los dispositivos. No se aceptarán dispositivos criptográficos cuya certificación FIPS haya sido otorgada solamente para el smartcard chip / micro-module / chip (ICC) que posea en su interior. Se deberá adjuntar el correspondiente documento "FIPS 140-2 Cryptographic Module Security Policy", el cual deberá estar emitido a nombre del Dispositivo Criptográfico Token USB

ofertado.

- Debe permitir implementar 'Doble Factor' de autenticación; es decir que es necesario a tal fin poseer la llave criptográfica y una contraseña. Soportando dos perfiles: Administrador y Usuario.
- Conectividad a través de los estándares Crypto API y PKCS#11.

Aplicaciones Soportadas:

- Windows logon
- Clientes Web: Microsoft Internet Explorer, Mozilla Firefox
- Clientes e-mail: Outlook, Outlook Express, Mozilla Thunderbird

Especificaciones Técnicas del producto:

- Plataformas soportadas: Windows 7, 8.1, 10, 2003/R2 Server, 2008/R2 Server, 2012/R2 Server, 2016 Server, Linux
- APIs y estándares soportados
  - PKCS#11 v2.01 o superior,
  - Microsoft Crypto API (CAPI) 2.0 o superior,
  - Microsoft PC/SC (Personal Computer Smart Card),
  - X.509 v3
  - SSL v3
  - IPSec/IKE
- Tamaño de memoria de al menos 80 Kbytes.
- Algoritmos de seguridad incorporados
  - Encriptación con claves asimétricas: RSA 1024-bit o superior.
  - Firma Digital: RSA 1024-bit y 2048 bits o superior.

- Generación de claves simétricas: 3DES (Triple DES),
- Algoritmo de Hash: SHA-1 y SHA-256

- Algoritmo de Generación Aleatoria de Números (RNG): La generación aleatoria de números debe realizarse por hardware e internamente en la llave criptográfica.
- Los dispositivos deberán contar con sus respectivas licencias de uso (de corresponder) y los correspondientes drivers y aplicativos necesarios para su funcionamiento en castellano.
- Deberá incluir una herramienta de administración para formatear los dispositivos en caso de ser necesario. La misma podrá ser independiente de los drivers de los dispositivos.
- **Garantía**: 2 años, in-situ

NOTA: El oferente deberá garantizar soporte técnico, así como también soporte de actualización de los drivers y firmware del dispositivo, sin costo alguno para el organismo, durante un período no inferior a 2 años a partir de la fecha de compra del mismo.

Similares prestaciones y características al eToken 5110 de la firma SafenetInc.

Ing. BARBERA, DANIELA
Subsecretaria de la Suprema Corte de Justicia
SUBSECRETARIA DE INFORMATICA DE LA PROCURACION GENERAL
Procuracion General
dbarbera@mpba.gov.ar