Estándares Tecnológicos para la Administración Pública

Dispositivos Criptográficos para Firma Digital – TOKEN

SEG-GDE

Dispositivos criptográficos con las siguientes características:

Presentación:

- Carcasa de protección compuesta de un material robusto.
- Características de 'tamper-evident'.
- Interfaz USB estándar tipo A, versión 2.0 o superior.
- Debe tener un LED indicador de actividad.

Características Técnicas:

- Debe permitir implementar 'Doble Factor' de autenticación, es decir que es necesario a tal fin poseer el dispositivo criptográfico y una contraseña.
- Autenticación interna (on-board).
- Permitir la obtención del número de serie del dispositivo criptográfico mediante la API PKCS# 11.
- Seleccionar una alternativa:
- Contar con certificación FIPS 140-2 Nivel 2 o superior, que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

Aplicaciones Mínimamente Soportadas:

- Windows logon (opcional)
- Clientes de e-mail:
  -Microsoft Outlook, Thunderbird.
- Navegadores:
  -Internet Explorer, Mozilla, Chrome.

Especificaciones Técnicas del producto:

- Sistema Operativos soportados:
  -Microsoft Windows 7/8/8.1 o superior y Microsoft Windows 2008 Server R2 o superior.
  -UNIX / 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),
- Tamaño de memoria de al menos 32 Kbytes.
- Deberá soportar las siguientes funciones criptográficas (on board)

-Algoritmo de Generación Aleatoria de Números (RNG):

- La generación aleatoria de números debe realizarse por hardware e internamente en el dispositivo.
- Los algoritmos de generación (RNG) deben estar aceptados en el listado del Anexo C, del “Approved Random Number Generators for FIPS PUB 140-2”.

-Generación interna, operación, almacenamiento y administración de claves criptográficas asimétricas del tipo RSA (mínimamente 2048).

-Generación de claves simétricas: Generación interna, y operación de claves criptográficas simétricas mínimamente AES.

-Almacenamiento de certificados X509v3.

-Capacidad de exportación de Certificados Digitales x509 v3.

-Algoritmo de Hash: Funciones de hash seguro, mínimamente “SHA-1 y SHA-2”.

Características administrativas y de uso:

- Los dispositivos deberán contar con sus respectivas licencias de uso (de corresponder) y los correspondientes drivers y aplicativos necesarios para su funcionamiento.
- Deberá contar con software asociado que permita definir usuarios comunes y formateo del dispositivo para restaurar a valores de fábrica.
- No deberá tener posibilidad de exportar la clave privada, ni hacer copias de la misma.

OTRAS:

Deberá ser un producto con homologación FIPS 140-2 Nivel 2 o superior vigente, con soporte técnico y no poseer fecha de discontinuidad de fabricación al momento de efectuarse la presentación.

El oferente deberá garantizar también soporte de actualización de los drivers del dispositivo, sin costo alguno para el organismo.

El oferente deberá brindar servicio de soporte a los usuarios poseedores de dispositivos.

Deberá tratarse de dispositivos criptográficos del fabricante cuya marca o fabricante y modelo y versión de hardware y firmware coincida con la marca o fabricante y modelo y versión de hardware y firmware declarada en las correspondiente Certificación FIPS 140, no pudiendo ser dispositivos criptográficos del tipo OEM (Original Equipment Manufacturer).

El oferente deberá entregar el software, los manuales y demás documentación, preferentemente en idioma español, o en su defecto, en idioma Inglés.