



Universidad Nacional de Luján

ANEXO 1

DISPOSITIVOS CRIPTOGRÁFICOS PARA FIRMA DIGITAL – TOKEN (APTO SISTEMA GDE)

Presentación:

Carcasa de protección compuesta de un material robusto.

Características de ‘tamper-evident’.

Interfase 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.

Contar con certificación FIPS 140-2 Nivel 2 o superior, que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

Aplicaciones Soportadas:

Windows logon (opcional)

Clientes de e-mail:

Microsoft Outlook, Thunderbird

Navegadores:

Internet Explorer, Mozilla, Chrome



Especificaciones Técnicas del producto:

Sistemas Operativos soportados (seleccionar una opción):

- Microsoft Windows 8.1/10 o superior y Microsoft Windows 2008/2013 Server 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 incluidos 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:

Mínimamente debe operar con claves RSA de al menos 2048 bits de longitud.

En caso de incluir algoritmo ECDSA, éste deberá operar con claves de al menos 224 bits de longitud.

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.



Universidad Nacional de Luján

Algoritmo de Hash: Funciones de hash seguro, mínimamente “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 entregar el software, los manuales y demás documentación, preferentemente en idioma español, o en su defecto, en idioma Inglés.

Garantía: Mínimo 12 meses.



ANEXO 2

ESCÁNERES DE HUELLAS UNI Y BIDACTILARES

DETALLE TÉCNICO / FUNCIONAL

Tipo de escáner: Unidactilar o Bidactilar

a Certificado del estándar “IAFIS image quality specification for scanners”, FBI CJIS-RS-0010 (V7) Apéndice F y publicado en

<https://www.fbibiospecs.org/IAFIS/Default.aspx>.

b Debe admitir tomas del tipo: Planas o Roladas. En este ultimo caso deberán contar con función anti-rollback, lo que impedirá que los pixeles capturados se sobrescriban ante un retroceso en la dirección de avance del dedo.

c Deberá permitir transmitir video en vivo de la imagen dactilar a capturar, a modo de feedback, al monitor de la estación de captura.

- El escáner deberá contar con capacidad de conectarse a un equipo X86 compatible a través de un puerto USB 2.0 o versión superior.

- La alimentación eléctrica del escáner será únicamente a través del puerto USB.

- Deberá incluir todos los cables necesarios para la comunicación de datos y alimentación del dispositivo.

- Deberá contar con los drivers necesarios para la correcta lectura de las imágenes capturadas bajo los siguientes sistemas operativos:

- Microsoft Windows.



Universidad Nacional de Luján

- Linux Debian/Ubuntu
- Deberá incluir los Kit de Desarrollo de Software (SDK) para desarrollos de aplicativos de software basados en DLLs, controles ActiveX u otra solución que pueda integrarse fácilmente a entornos de desarrollo .NET, Java, etc.
- Modelo similar a Lector biométrico U Are U 4500 usb.
- Garantía: mínimo 12 meses.



ANEXO 3

Camara Web para captura de datos faciales

Características

- Resolución máxima de vídeo: 1920 x 1080
- Tipo de resolución máxima de video: Full HD
- Interfaces: USB-A 2.0
- Funciones: Micrófono incorporado
- Es apto para videoconferencia: Sí
- Sistemas operativos mínimos requeridos: Windows 8, Linux
- Cuadros máximos por segundo: 60 FPS
- Zoom: 1x
- Dispositivos recomendados: PC de escritorio, Notebook
- Accesorios incluidos: Clip con montaje en trípode, Trípode, Manual de usuario, Licencia premium de XSplit por 3 meses
- d Aplicaciones compatibles: OBS, XSplit
- e Ángulo de visión: 78°
- Es plug and play: Sí
- Largo del cable: 1.5 m
- Garantía: 12 meses