Ministerio de Modernización
Presidencia de la Nación

Código ETAP: SEG-002-00

Dispositivos Criptográficos para Firma Digital – TOKEN (apto sistema GDE)

ETAP Versión 22

Realizado por:
Pablo Ferrante

Índice

1. Vista General de documento

Este documento permitirá agilizar la intervención técnica que realiza la Dirección de Estandarización Tecnológica (DET) en su función de participar en todos los proyectos de innovación tecnológica que abarca, entre otras, la adquisición, implementación, incorporación, e integración de las tecnologías de información en el ámbito del sector público.

En la sección 3, obran las especificaciones técnicas estándares.

El resto del documento y las notas agregadas dentro de recuadros en las especificaciones, contienen comentarios de ayuda, para que los organismos puedan completar fácilmente las especificaciones, seleccionando las características técnicas de los equipos y/o servicios en función de sus necesidades funcionales, por lo que, dichas notas de ayuda y comentarios, no deben ser transcriptas en la especificación final.

En las especificaciones técnicas hemos incluido características y elementos del recurso y/o servicio tecnológico que se detalla, que son ***de inclusión mandatoria*** por entender que los mismos resultan indispensables. Por lo cual, esperamos encontrarlos incluidos en el requerimiento técnico elevado para la intervención.

También hemos incluido características y elementos que son ***opcionales*** en la definición del recurso tecnológico y/o servicio que se detalla, los cuales deberán seleccionarse de acuerdo a sus necesidades funcionales. Para esto se usan “checkboxes” y “radio-buttons”, lo que facilita diferenciar entre grupos de opciones de selección libre, y grupos de opciones de selección mutuamente excluyente, respectivamente.

En ambos casos, describimos o definimos varias características y/o elementos, para que los organismos seleccionen las que más se ajusten a sus necesidades. En consecuencia, una vez que se seleccione la o las características y/o elementos deseados, las opciones no seleccionadas deberán eliminarse de la especificación.

El documento cuenta con 3 secciones:

Sección	Tema desarrollado en la sección
Vista General	La sección de *vista general de documento* detalla la forma de uso y las secciones que componen este documento.
Descripción del Estándar	Esta sección provee una breve Descripción del Estándar que se va a especificar.
Especificación Técnica	La sección de *Especificación Técnica* detalla las características generales y particulares del recurso tecnológico o servicio.

2. Descripción del Estándar

Dispositivos Criptográficos para Firma Digital – TOKEN (aptos para el sistema GDE).

3. Especificación Técnica - SEG-002-00 Dispositivos Criptográficos para Firma Digital – TOKEN (apto sistema GDE)

Esta sección provee el detalle técnico del recurso tecnológico definido en la descripción del estándar.

3.1 Características Generales

Dispositivos criptográficos con las siguientes características:

- 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.

3.2 Detalle Técnico / Funcional

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".

a) Aplicaciones Soportadas:

Windows logon (opcional)

Clientes de e-mail:

Microsoft Outlook, Thunderbird

Navegadores:

Internet Explorer, Mozilla, Chrome

b) Especificaciones Técnicas del producto:

Sistemas Operativos soportados (seleccionar una opción):

- Microsoft Windows 8.1/10 o superior y Microsoft Windows 2008/2013 Server R2 o superior.
- MAC OS-X 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 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".

c) 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.

d) 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.