ANEXO II - RESOLUCION GENERAL Nº 2674

CARACTERISTICAS DE LOS DISPOSITIVOS CRIPTOGRAFICOS A HOMOLOGAR

1. Satisfacer los requerimientos técnicos de la ETAP "Elementos de Seguridad – SEG-E" en su última versión.

2. Permitir la obtención del número de serie del dispositivo criptográfico mediante la API PKCS# 11.

3. Contar con certificación FIPS 140 (Versión 1 ó 2) Nivel 2 o superior que incluya todo el conjunto de "Software", "Firmware" y "Hardware".

4. Autenticación interna (on-board).

5. Conexión USB estándar tipo A, versión 1.1 o superior.

6. Soportar los siguientes estándares: PKCS#11 versión 2.01 o superior, CAPI (Microsoft Crypto API), PC/SC.

7. Poseer memoria de almacenamiento de datos mínima de 32 kbytes.

8. Soportar las siguientes funciones criptográficas:

8.1. Generación de números aleatorios (RNG).

8.2. Almacenamiento de certificados X509v3.

8.3. Generación interna, operación, almacenamiento y administración de claves criptográficas asimétricas del tipo RSA (1024 bits o superior).

8.4. Funciones de hash seguro del tipo SHA-1.

8.5. Generación interna, operación de claves criptográficas simétricas del tipo DES y/o Triple DES.

9. Ser un producto vigente, con soporte técnico y no poseer fecha de discontinuidad de fabricación al momento de efectuarse la presentación de solicitud de homologación.

10. Deberá tratarse de dispositivos criptográficos del fabricante cuya marca y modelo coincida con la marca y modelo declarada en las correspondientes Certificaciones FIPS 140, no pudiendo ser dispositivos criptográficos del tipo OEM (Original Equipment Manufacturer).

11. Brindar servicio de soporte a los usuarios poseedores de dispositivos.