RA21: CONDICIONES MÍNIMAS DE SEGURIDAD QUE DEBEN REUNIR LOS DISPOSITIVOS TOKEN

Especificaciones técnicas:

- Implementación nativa USB. El token debe tener una conexión nativa USB, sin necesidad de utilizar lectores separados ni otro tipo de conexión física diferente de USB.
- Cumplimiento con el estándar ISO 7816 1-2-3-4. El ISO 7816 es el estándar para Smart Cards. El token escogido debe cumplir con este estándar para garantizar la ausencia de problemas de compatibilidad entre dispositivos físicos y aplicaciones de software.
- Propia Generación de llaves. El token debe poder realizar operaciones criptográficas que generen la llave privada y pública que serán asociadas al certificado digital. Así mismo, debe garantizar la protección de la llave privada almacenada en el token.
- Algoritmos 3DES y RSA (1024 bits). Para garantizar la máxima seguridad disponible, el token debe poder utilizar los algoritmos 3DES y RSA, ambos reconocidos por su seguridad y confiabilidad. Algoritmos viejos o inseguros como DES no deben ser permitidos. El token debe tener la capacidad de generar y almacenar llaves de 1024 bits.

  Menos de esto compromete los requerimientos de Seguridad del Ministerio.
- Firma RSA (512-1024 bits) y SHA-1. El token debe poder utilizar una implementación de la firma RSA de 512 a 1024 bits y del algoritmo SHA-1.
- Memoria ROM: 96k, RAM: 4k, EEPROM: 32k. El token debe tener estas especificaciones de memoria para garantizar un espacio de almacenamiento de certificados aceptable y una buena velocidad de operación.
- CPU de 8-bit. Un procesador de este tipo permite la ejecución rápida de operaciones criptográficas, aspecto que es fundamental en el uso de token USB. Un token lento tendrá impacto negativo fuerte en operaciones para la generación y la renovación de certificados.
- 10 años de retención de datos. El token debe garantizar la retención de la información que tiene almacenada por un período de 10 años (bajo condiciones normales de operación de un token USB).
- Rendimiento EEPROM mayor a 400.000 ciclos de lectura/escritura. Un daño en la memoria EEPROM del token lo dejará inservible para realizar operaciones indispensables para su funcionamiento. Por esto, el fabricante del token debe garantizar que la memoria EEPROM que utiliza el token soporta más de 400.000 ciclos de lectura/escritura dentro de la vida útil del token.
- Contactos físicos ISO 7816-2, cumplimiento con el estándar mencionado anteriormente en el aspecto de comunicaciones.

- Junto con el token se debe adquirir los “drivers” correspondientes de instalación. Dicha instalación debe realizarla el interesado bajo su responsabilidad.
- El token a adquirir deberá ser compatible con alguna de las siguientes marcas: Alladin, Rainbow, las cuales cumplen con los requerimientos solicitados.
- El dispositivo debe cumplir con los estándares de seguridad Certificación FIPS 140-1 nivel 2.

Ejemplos de dispositivos token permitidos y no permitidos:

<table>
<tr><th colspan="4">Ejemplos de dispositivos token permitidos
(Cumplen con el FIPS o nivel de seguridad mínimo requerido)</th></tr>
<tr>
<td>SafeNet iKey 4000 Authentication Token.

</td>
<td>De los iKey 2032 en el modelo nuevo, todos son FIPS. SafeNet iKey 2032 Authentication Token.

</td>
<td>De los ikey 2032 Raimbow modelo viejo, color negro.
 </td>
<td>Alladin color azul, morado o rojo.
 </td>
</tr>
<tr><th colspan="4">Ejemplos de Tokens NO Permitidos
(NO cumplen con el FIPS o nivel de seguridad mínimo requerido)</th></tr>
<tr>
<td>SafeNet iKey 1000 Authentication Token

</td>
<td>SafeNet iKey 2032 Authentication Token, color morado.
 </td>
<td>SafeNet iKey 2032 Authentication Token, color gris.
 </td>
<td>SafeNet iKey 2032 Authentication Token, color rojo.
 </td>
</tr>
</table>

Todos aquellos usuarios o suscriptores que posean dispositivos que **NO** cumplan con lo indicado, apersonarse al Departamento de Estadística y Registros con el nuevo dispositivo, para que se les haga nueva entrega de los certificados.

Para mayor información sírvanse llamar a los teléfonos: **2522-9090**, **2522-9097**, **2522-9098** y **2522-9099**, a la Autoridad Certificadora, teléfono **2257-9055**, extensiones **160** y **246** o a la dirección electrónica Autoridad-Certificadora@hacienda.go.cr .

Empresas Proveedoras de los Dispositivos TOKEN

Empresa	Contacto	Marca	Teléfono	E-mail
Identiga	Luis Cordero	Rainbow	221-18-21	lcordero@identiga.com
It-SecurityServices	Vicente Ramírez	Aladdin	258-34-94	vicente_ramirez@ it-securityservices.com
Componentes El Orbe	Sonia Vega	Rainbow	297-11-11 Ext 223	svega@orbe.co.cr