

Equipos de Seguridad Tokens

Se requiere de estos dispositivos para almacenar certificados digitales.

| | CARACTERISTICAS | ESPECIFICACION REQUERIDA | ESPECIFICACION SOLICITADA |
|-----|--|--|---------------------------|
| 1. | Sistema Operativo Microsoft | Windows 98SE, ME, Windows2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server2008 | Mínimo |
| 2. | Sistema Operativo Linux | Debian 3.1 y superior, Redhat 9 y superior, Redhat Enterprise 4, 5 y superior Fedora 5, 6 y superior SUSE10 y superior, OpenSuSe Ubuntu 5.04 & 5.10, 7.04 y superior | Mínimo |
| 3. | API & Soporte Standard | PKCS#11 v2.11, CAPI (Microsoft Crypto API) X.509 v3 certificate storage, SSLv3, IPSec/IKE, Compatibilidad ISO 7816 | Mínimo |
| 4. | Software Developer kit | Microsoft y Linux | Mínimo |
| 5. | Tamaño de memoria | 32Kb | Mínimo |
| 6. | ID de Hardware | El dispositivo deberá proveer un smartcards ID de 64 bits para identificación en aplicaciones. | Mínimo |
| 7. | Identificación serial | Los dispositivos criptográficos deben tener una identificación única externo para una identificación fehaciente por parte del organismo, para poder administrar los dispositivos y poder inventariar físicamente los mismos. | Mínimo |
| 8. | Carcasa | Carcasa endurecida anti-forzados | |
| 9. | Algoritmos de Seguridad On-Board: | RSA 1024-bit | Mínimo |
| 10. | Mecanismo de Encriptación Autenticación en el chip (onboard) | RSA 1024-bit, DES, 3DES (Triple DES) | Mínimo |
| 11. | Algoritmos de hash | SHA1 y MD5 | Mínimo |
| 12. | Generación de números | Random number generation on board | Mínimo |
| 13. | Conexión | USB type A (Universal Serial Bus) | Mínimo |
| 14. | Retención de datos | Al menos 10 años | Mínimo |
| 15. | Reescritura de memoria | Al menos 100.000 veces | Mínimo |
| 16. | Herramientas de Administración Windows | El software asociado y las herramientas de administración para todas las plataformas solicitadas deberá estar en castellano | Mínimo |

| | | | |
|-----|--|--|---------|
| 17. | Certificados Digitales | Poder almacenar Certificados X.509 v3 e importar certificados digitales y sus llaves publicas y privadas | Mínimo, |
| 18. | Resguardo de los certificados digitales | El dispositivo no puede permitir exportar la clave privada del certificado, ni hacer copias de backup. | Mínimo, |
| 19. | Herramienta de Administración de Windows o Linux | La herramienta debe permitir importar certificados de tipo, .P12; .PFX; .PB7; .Cer. | Mínimo, |
| 20. | Manuales | Castellano | Mínimo |
| 21. | Licenciamiento de software | Perpetuo | Mínimo |
| 22. | Actualizaciones de Software | Sin cargo | Mínimo |
| 23. | Formateo | Se deberá proveer una herramienta de formateo de los dispositivos (smartcard usb) para restaurar la configuración de fabrica (Set to Factory) sin comprometer la seguridad y además recuperar el dispositivo (token usb) para retornarlo a producción en el organismo. | Mínimo |
| 24. | Instalacion | Se deberá proveer un instalador independiente para los drivers de los dispositivos y el mismo no deberá instalar ninguna herramienta de administración (ni para el usuario ni para el administrador) | Mínimo, |
| 25. | Autenticación | El dispositivo debe proveer autenticación a través de PIN, soportando 2 perfiles (Administrador y Usuario) | Mínimo |
| 26. | LED | Indicador de Actividad. | Mínimo |
| 27. | Herramientas de Administración LINUX | Castellano | Mínimo |
| 28. | Cliente de correo | Soporte para Outlook, Outlook Express, Mozilla Thunderbird, Groupwise, Windows Mail | Mínimo |
| 29. | Browser | Soporte para Internet Explorer, Netscape, Mozilla Firefox | Mínimo |
| 30. | Identificación serial externa impresa en Hardware para control | Número serial de la partida, generando un identificador único visible | Mínimo |
| 31. | Guías de Integración | Se deben proveer guías de integración para que los usuarios finales puedan seguir paso a paso. Las mismas explicando los procedimientos de uso token y la interacción con diferentes browsers y clientes de correo Thunderbird, Firefox, Outlook y Outlook Express, Windows Mail, como mínimo. | Mínimo |
| 32. | Restringir token virtual | No se admitirá una solución que provea tokens virtuales | |