SafeNet eToken 5110

Para proteger las identidades y las aplicaciones comerciales críticas en el entorno empresarial digital actual, las organizaciones deben garantizar que el acceso a los recursos en línea y de la red sea siempre seguro, al tiempo que cumplen con las regulaciones en materia de seguridad y privacidad. SafeNet eToken 5110 ofrece la autenticación de dos factores (2FA) para un acceso remoto y de red seguro, así como el soporte basado en **certificados para aplicaciones de seguridad avanzadas, incluida la firma digital y la autenticación previa al arranque.**

Autenticación de dos factores en la que puede confiar

SafeNet eToken 5110 es un autenticador USB portátil de dos factores con tecnología avanzada de tarjetas inteligentes. **La tecnología basada en certificados genera y almacena** credenciales, tales como claves privadas, contraseñas y **certificados digitales dentro del entorno protegido del chip** de la tarjeta inteligente. Para autenticarse, los usuarios deben proporcionar tanto su autenticador personal SafeNet eToken como su contraseña, lo que proporciona un segundo nivel crítico de seguridad más allá de las contraseñas simples y de ese modo proteger los valiosos recursos comerciales digitales.

A prueba del futuro y del crecimiento con Control de Gestión Centralizada

SafeNet eToken 5110 se basa en la plataforma avanzada IDCore de Thales y se integra perfectamente con aplicaciones de terceros a través de las herramientas de desarrollo de autenticación SafeNet, es compatible con el PKI de SafeNet, así como aplicaciones de gestión de contraseñas y herramientas de desarrollo de software; además, permite la personalización de aplicaciones y la extensión de la funcionalidad a través de subprogramas Java integrados. SafeNet eToken 5110 es también compatible con SafeNet Authentication Client para gestión local completa y soporte para administración, eventos e implementación avanzada de tokens.

Beneficios

- Mejora la productividad al permitir que los empleados y socios accedan de forma segura a los recursos corporativos.
- **Habilita aplicaciones avanzadas basadas en certificados, tales como la firma digital y la autenticación previa al arranque**
- Token USB portátil: no se necesita un lector especial
- Sencillo y fácil de usar: no se necesita capacitación ni conocimientos técnicos
- Expande las aplicaciones de seguridad a través de subprogramas Java integrados
- Mejora las iniciativas de marketing y marca con etiquetas privadas y opciones de color

Aplicaciones compatibles

- Acceso remoto seguro a VPNs y portales web y a servicios en la nube
- Inicio de sesión seguro en la red
- Firma digital
- Autenticación previa al arranque

Especificaciones técnicas

Sistemas operativos compatibles	Windows Server 2008/R2, Windows Server 2012 y 2012 R2, Windows 7, Mac OS, Linux, Windows 8, Windows 10, Windows 11		
Soporte para estándares y para interfaces de programación de aplicaciones (API)	**PKCS#11, Microsoft CAPI, PC/SC, almacenamiento de certificados X.509 v3, SSL v3, IPSec/IKE,** minicontrolador MS, CNG		
Tamaño de la memoria	80K		
Dimensiones	5110– 16.4mm*8.5mm*40.2mm		
Asistencia para especificación ISO	**Asistencia para especificaciones ISO 7816-1 a 4**		
Temperatura de operación	0° C a 70° C (32° F a 158° F)		
Temperatura de almacenamiento	-40° C a 85° C (-40° F a 185° F)		
Clasificación de humedad	0 - 100% sin condensación		
Certificación de resistencia al agua	IP X7 – IEC 60529		
Conector USB	USB tipo A; admite USB 1.1 y 2.0 (velocidad máxima y alta velocidad)		
Cubierta	Plástico moldeado duro, a prueba de manipulaciones		
Retención de datos de memoria	Al menos 10 años		
Reescrituras de las células de memoria	Al menos 500.000		
	SafeNet eToken 5110 FIPS	**SafeNet eToken 5110 CC**	**SafeNet eToken 5110**
Algoritmos de seguridad a bordo	• Simétrico: AES, 3DES (Triple DES) 128/192/256 bit • Hash: SHA-256 • RSA: 2048 bits, • Curvas elípticas: P-256, P-384, ECDH	• Simétrico: 3DES (ECB, CBC), AES (128, 192, 256 bits) • Hash: SHA-1, SHA-256, SHA-384, SHA-512 • RSA: RSA hasta 4096 bits • RSA OAEP y RSA PSS • P-256 bits ECDSA, ECDH. • P-384 & P-521bits • ECDSA, ECDH están disponibles **a través de una configuración** personalizada • Generación de pares de claves asimétricos en la tarjeta (RSA hasta 4096 bits y curvas elípticas hasta 521 bits) • Simétrico: AES: para mensajería segura y 3DES solo para protocolos desafío-respuesta de Microsoft	• Simétrico: 3DES (Triple DES), AES 128/192/256 bit • Hash: SHA1, SHA256 • RSA 1024 bits / 2048 bits • Curvas elípticas: P-256, P-384, ECDH
Certificaciones de seguridad	FIPS 140-2 Nivel 3	CC EAL5+ / PP QSCD, eIDAS **calificado para eSignature y eSeal, y calificado por la ANSSI francesa**	FIPS 140-2 nivel 3 (chip SC y SO)
Plataforma de tarjeta inteligente	Thales IDCore 30 (rev B) y eToken applet	IDPrime MD 940	Thales IDCore 30 y eToken applet