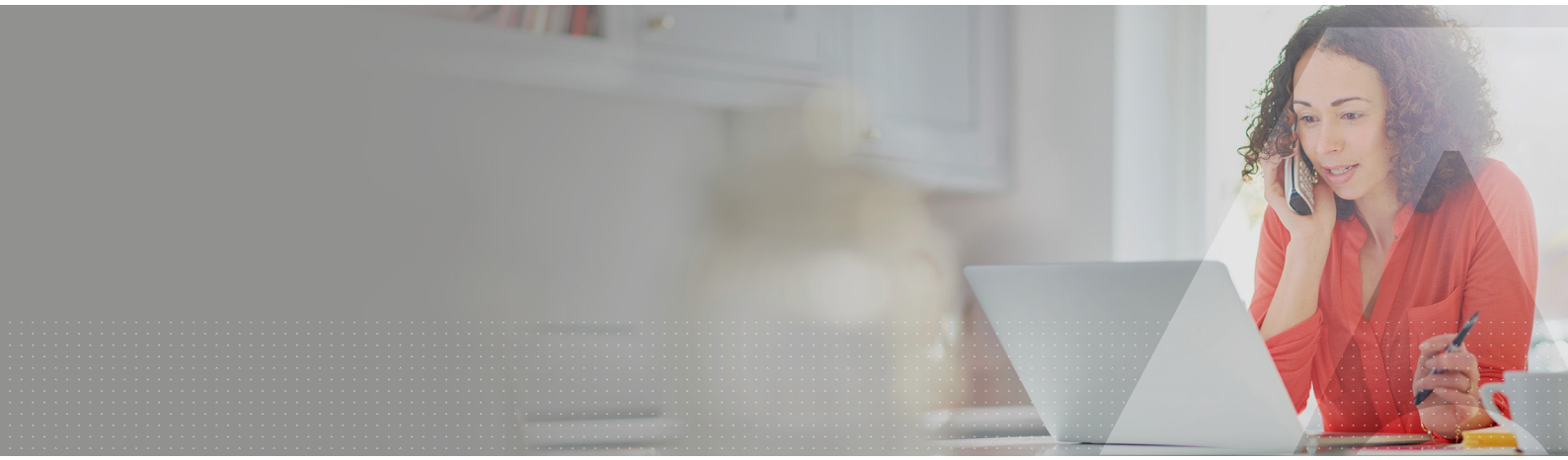
cpl.thalesgroup.com/fr

THALES
Building a future we can all trust

Série SafeNet eToken 5110



Pour protéger les identités et les applications essentielles des entreprises dans l'environnement numérique actuel, les organisations doivent garantir la sécurité ininterrompue des accès aux ressources en ligne et réseau, tout en maintenant leur conformité aux réglementations de sécurité et de confidentialité. SafeNet eToken 5110 offre une authentification à deux facteurs pour un accès sécurisé à distance et au réseau, ainsi qu'une prise en charge des applications de sécurité avancées basée sur les certificats, y compris la signature numérique et l'authentification avant démarrage.

Une authentification à deux facteurs fiable

SafeNet eToken 5110 est un dispositif d'authentification USB à deux facteurs portable doté de la technologie de carte à puce avancée. La technologie basée sur les certificats génère et stocke des identifiants tels que les clés privées, les mots de passe et les certificats numériques dans l'environnement protégé de la puce de la carte. Pour s'authentifier, les utilisateurs doivent fournir leur dispositif d'authentification personnel SafeNet eToken et leur mot de passe, ce qui permet d'obtenir un deuxième niveau crucial de sécurité au-delà des mots de passe simples, afin de protéger les ressources numériques essentielles des entreprises.

Avantages

- Amélioration de la productivité en permettant un accès sécurisé aux ressources de l'entreprise pour les employés et les partenaires
- Prise en charge des applications de sécurité avancées basées sur les certificats, telles que la signature numérique et l'authentification avant démarrage
- Token USB portable : ne nécessite aucun lecteur spécial
- Simple d'utilisation : ne nécessite aucune formation ni aucune expertise
- Mettez en valeur les initiatives marketing et de marque avec des options de personnalisation d'étiquetage et de palette de couleurs

Applications prises en charge

- Authentification à deux facteurs robuste (résistante aux attaques d'hameçonnage)
- Accès à distance sécurisé aux VPN et aux portails Web
- Connexion sécurisée au réseau
- Chiffrement des e-mails
- Signature numérique
- Authentification avant démarrage

Caractéristiques techniques

	SafeNet eToken 5110+ FIPS	SafeNet eToken 5110+ CC	SafeNet eToken 5110+
Prise en charge des API et des standards	• Minipilote BaseCSP (minipilote SafeNet) • Global Platform 2.2.1 • Java Card 3.05 • ISO 7816	• Minipilote BaseCSP (minipilote SafeNet) • Global Platform 2.2.1 • Java Card 3.04 • ISO 7816	• Minipilote BaseCSP (minipilote SafeNet) • Global Platform 2.2.1 • Java Card 3.04 • ISO 7816
Taille de la mémoire	78 Ko	73 Ko	80 Ko
Systèmes d'exploitation pris en charge	Windows, MAC, Linux		
Dimensions	5110 : 16,4 mm x 8,5 mm x 40,2 mm		
Prise en charge des spécifications ISO	Prise en charge des spécifications ISO 7816-1 à 4		
Température de fonctionnement	de 0 à 70 °C (de 32 à 158 °F)		
Température de stockage	de -40 à 85 °C (de -40 à 185 °F)		
Taux d'humidité	De 0 à 100 % sans condensation		
Certification de résistance à l'eau	IP X7 – IEC 60529		
Prise USB	USB type A, prend en charge USB 1.1 et 2.0 (débit total et haut débit)		
Boîtier	Plastique moulé rigide, inviolable		
Rétention des données de la mémoire	Au moins 10 ans		
Réécritures des cellules de mémoire	Au moins 500 000		
Algorithmes de sécurité embarqués	• Symétrique : AES, pour une correspondance sécurisée, et 3DES pour l'authentification par stimulation/réponse de Microsoft uniquement • Hachage : SHA-1, SHA-256, SHA-384, SHA-512. • RSA : jusqu'à RSA 4 096 bits • RSA OAEP et RSA PSS • ECDSA P-256 bits, ECDH. ECDSA, P-384 et P-521 bits, ECDH • Génération de paires de clés asymétriques sur carte (RSA jusqu'à 4 096 bits et courbes elliptiques jusqu'à 521 bits)	• Symétrique : AES, pour une correspondance sécurisée, et 3DES pour l'authentification par stimulation/réponse de Microsoft uniquement • Hachage : SHA-1, SHA-256, SHA-384, SHA-512 • RSA : jusqu'à RSA 4 096 bits • RSA OAEP et RSA PSS • ECDSA P-256 bits, ECDH. ECDSA, P-384 et P-521 bits et ECDH sont disponibles par le biais d'une configuration personnalisée • Génération de paires de clés asymétriques sur carte (RSA jusqu'à 4 096 bits et courbes elliptiques jusqu'à 521 bits)	• Symétrique : 3DES (Triple DES), AES 128/192/256 bits • Hachage : SHA1, SHA256 • RSA : jusqu'à RSA 2 048 bits • Courbes elliptiques : P-256, P-384, ECDH
Certifications de sécurité	FIPS 140-2 (en attente de l'examen du NIST)	Qualification CC EAL5+/PP QSCD et eIDAS pour eSignature et eSeal, et qualification par l'agence ANSSI française	Certification de carte à puce CC EAL6+
Plateforme de carte à puce	IDPrime 930	IDPrime 940	Applet IDCore 30 et eToken de Thales