ePass2003

Jeton d'authentification PKI
Version R6 - FIPS niveau 3

KORUM SECURE
korum-secure.com

Signature et chiffrement des e-mails

Ouverture de session Windows avec carte à puce

Signature numérique de document

Transaction en ligne sécurisée

Chiffrement des disques et des fichiers

Accès VPN à distance

KORUM SECURE
korum-secure.com

FEITIAN
WE BUILD SECURITY

Le FEITIAN ePass2003 est un jeton USB PKI de haute sécurité intégrant les technologies et standards cryptographiques les plus puissants disponibles aujourd'hui. Il est conçu pour tous les environnements d'Infrastructure à Clés Publiques (PKI) et apporte une authentification cryptographique à deux facteurs aux applications où la sécurité est critique.

Le système d'exploitation de carte validé FIPS 140-2 et niveau 3 compatible ainsi que le mécanisme intégré de gestion des clés permettent d'assurer un niveau de sécurité plus élevé pour un large éventail d'applications sensibles.

Grâce à sa compatibilité combinée avec Microsoft Minidriver et OpenSC, l'ePass2003 est compatible avec les applications fonctionnant sous Windows, Linux et Mac, ce qui en fait le choix idéal pour tous les secteurs nécessitant une protection de haut niveau, tels que les administrations, les entreprises, les institutions financières et les sociétés de médias.

Entreprise

Les entreprises doivent non seulement sécuriser leurs réseaux, mais aussi signer numériquement leurs documents et leurs e-mails. Au lieu d'utiliser plusieurs dispositifs, l'ePass2003 fait tout cela en un seul appareil. L'ePass2003 fonctionne avec Microsoft Office pour la signature de documents, permet l'ouverture de session par carte à puce, et est compatible avec une gamme de fournisseurs de VPN tels que CheckPoint VPN, afin de garantir que votre réseau reste sûr et sécurisé. Avec la prise en charge des interfaces CSP et PKCS#11, vous avez la certitude que l'ePass2003 est compatible avec vos applications.

Édition et médias

Dans le monde de l'édition et des médias, livrer du contenu de manière sécurisée aux clients est essentiel pour protéger le retour sur investissement (ROI). Avec la prise en charge de Windows EFS, PGP et d'autres formats majeurs de chiffrement de fichiers, les médias peuvent être distribués rapidement et facilement, en ligne comme hors ligne, sans crainte de vol de droits d'auteur. L'ePass2003 est également compatible avec tous les principaux navigateurs Internet tels que Microsoft Edge, Firefox, Chrome, Safari et Internet Explorer, garantissant ainsi que vos contenus atteignent le plus large public possible. Nous disposons également d'outils de gestion des certificats, incluant l'importation, l'exportation et la suppression.

Gouvernement

L'ePass2003 est un jeton répondant aux normes les plus exigeantes.Conforme aux certifications FIPS 140-2, niveau 3 en cours de certification et Common Criteria EAL 5+ (au niveau de la puce), l'ePass2003 est parfaitement adapté aux solutions gouvernementales telles que la déclaration d'impôts ou les procédures judiciaires. À l'ère numérique, où les gouvernements s'orientent vers des processus sans papier afin de réduire les coûts, de protéger l'environnement et d'accroître l'efficacité, l'ePass2003 constitue le remplaçant idéal de la signature manuscrite.

Finance

En finance, la confiance est primordiale. Afin de garantir la sécurité des finances de millions de clients dans le monde, il est essentiel d'utiliser un jeton offrant le plus haut niveau de sécurité du marché.

Avec les algorithmes de sécurité avancés RSA 2048 bits, AES 256 et SHA-2, les transferts en ligne des clients peuvent être protégés. Grâce à la prise en charge des connexions SSL, norme de l'industrie en matière de connexions sécurisées, chaque échange est assuré d'être protégé.

L'ePass2003 est également flexible grâce à sa grande capacité mémoire, qui lui permet de stocker de nombreux certificats et donc d'être utilisé avec plusieurs comptes et applications..

Spécifications

Systèmes d'exploitation supportés	Windows 2000 / XP / Server 2003 / Vista / Server 2008 /Server 2008 R2 / 7 / Server 2012 / Server 2012 R2 / 8 / 8.1 / 10, Linux, macOS
Interface matériel	ISO 7816-1, 2, 3, 4 compatible, CCID
API standards	PKCS# 5, 7, 8, 10, 11, 12 Supported Cryptographic Service Provider (CSP) Microsoft Smart Card Minidriver Microsoft CNG, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, CSR Export
Certifications	FIPS 140-2 Level 2 & Level 3 compatible certification en cours

Algorithmes de cryptage	Asymmetric Key: PKCS#1 V2.2 Onboard Key Pair Generation RSA 1024/2048/3072/4096 bit (RSAES-OEAP, RSASSA-PSS) Key generation time-For RSA 1023/2048/3072: Seconds; For RSA4096: less than a Minute. ECC 192/256/384/521 ECDSA 192/256 bit Symmetric Key: DES(NON-FIPS Mode)/3DES AES 128/192/256 bit Digest: SHA-1, SHA-2 SHA-256, SHA-384, SHA-512, SHA512/224, SHA-512/256
Caractéristiques	Secure MCU: 8/16/32 bits Memory Space: 64 KB Connectivity: USB 1.1/2.0/3.0 compliant Standards: CE, FCC, RoHS Data Retention: at least 10 years Flash Memory: Up to 4MB, enable autorun function USB connectors durability: ≥2,500 plug-unplug cycles Operating: 0°C~50°C Storage: -20°C~60°C Humidity: 0~100% RH

KORUM SECURE
korum-secure.com

www.korum-secure.com

Email contact@korum-secure.fr

FTC(XX)