

# Tokens PKI

## Authentification, cryptage et signatures numériques

### Tokens matériels PKI

Les tokens PKI sont des équipements matériels qui stockent, de manière sécurisée, des certificats numériques et des clés privées. Lorsque vous devez crypter, décrypter ou signer quelque chose, le token exécute la tâche en interne sur une puce sécurisée. Les clés ne courent donc jamais le risque d'être volées.

Nous proposons les tokens PKI, suivants :



#### ePass2003 USB PKI Token

#### Carte à puce PKI

Description	Le Feitian ePass2003 est un jeton certifié FIPS 140-2 de niveau 3 qui permet le stockage sécurisé des informations d'identité personnelles, des certificats numériques et des clés privées pour l'authentification, le cryptage et les signatures numériques. Ce jeton USB PKI standard est très apprécié au niveau international	Stockage sécurisé d'informations d'identité, de certificats numériques et de clés privées au sein d'une carte de format ID-1. Supporte le cryptage/décryptage et les signatures numériques. Compatible NFC pour les applications sans contact. Peut être utilisé avec n'importe lequel de nos Lecteurs de cartes à puce
Fonctions	<ul style="list-style-type: none"><li>• Connectivité USB</li><li>• Génération de clés intégrée</li><li>• Signature et vérification de signatures numériques intégrées</li><li>• Cryptage et décryptage de données intégrés</li><li>• PKCS#11 v2.40 avec prise en charge du cryptage OEAP / PSS</li><li>• PKCS#15</li><li>• Stockage de certificat X.509 v3</li><li>• Compatible OpenSC</li></ul>	<ul style="list-style-type: none"><li>• Fonctionnement NFC sans contact (ISO/IEC 14443)</li><li>• Génération de paires de clés RSA intégrée</li><li>• Signature et vérification de signatures numériques intégrées</li><li>• Cryptage et décryptage de données intégrés</li><li>• PKCS#11 v2.40 avec prise en charge du cryptage OEAP / PSS</li><li>• PKCS#15</li><li>• Stockage de certificat X.509 v3</li><li>• Compatible OpenSC</li></ul>
API et protocoles supportés	<ul style="list-style-type: none"><li>• Microsoft CAPI, GNC</li><li>• Generic Identity Device Specification (GIDS)</li><li>• PKCS#11 v2.40</li><li>• Microsoft Smart Card Minidriver</li><li>• PC/SC CCID</li><li>• SSL v3</li><li>• IPSec/IKE</li></ul>	<ul style="list-style-type: none"><li>• Microsoft CAPI, GNC</li><li>• Generic Identity Device Specification (GIDS)</li><li>• PKCS#11 v2.40</li><li>• Microsoft Smart Card Minidriver</li><li>• PC/SC, CCID</li><li>• SSL v3</li><li>• IPSec/IKE</li></ul>
Algorithmes	<ul style="list-style-type: none"><li>• RSA 1024/2048 bit (RSAES-OEAP, RSASSA-PSS)</li><li>• ECDSA 192/256 bits (optionnel)</li><li>• DES/3DES</li><li>• AES 128/192/256 bits</li><li>• SHA-1, SHA-2, MD5</li></ul>	<ul style="list-style-type: none"><li>• RSA 1024/2048 bits</li><li>• ECDSA 192/256 bits (optionnel)</li><li>• DES/3DES</li><li>• AES 128/192/256 bits</li><li>• SHA-1, SHA-2, MD5</li></ul>

Caractéristiques	<ul style="list-style-type: none"> <li>• Conforme ISO-7816</li> <li>• Mémoire : 64 Ko</li> <li>• Conservation de données 10 ans +</li> <li>• Température de fonctionnement : 0 °C ~ 50 °C</li> <li>• Température de stockage : -20 °C ~ 60 °C</li> <li>• Humidité : 0 ~ 100 % HR</li> </ul>	<ul style="list-style-type: none"> <li>• Java Card 2.2.2</li> <li>• Global Platform 2.1.1</li> <li>• Conforme ISO-7816</li> <li>• Conforme ISO/IEC 14443</li> <li>• Puce : Infineon SLE77CLFX2400PM</li> <li>• Tension de fonctionnement : 3 V/5 V</li> <li>• Mémoire : 68 Ko</li> <li>• 500 000+ réécritures de la mémoire</li> <li>• Conservation de données 10 ans +</li> </ul>
Systèmes d'exploitation compatibles	<ul style="list-style-type: none"> <li>• Windows PC/Portable</li> <li>• macOS</li> <li>• Linux</li> </ul>	<p>La carte à puce PKI prend en charge les systèmes d'exploitation suivants et nécessite un lecteur compatible</p> <ul style="list-style-type: none"> <li>• Windows PC/Portable</li> <li>• macOS</li> <li>• Linux</li> <li>• iPhone</li> <li>• iPad</li> <li>• Tablette Windows</li> <li>• Android (sans contact (NFC), ou par l'intermédiaire d'un lecteur compatible)</li> </ul>
Certifications	<ul style="list-style-type: none"> <li>• CC EAL 5 + (puce)</li> <li>• Conforme CE, FCC, RoHS</li> <li>• Certifié FIPS 140-2 niveau 3</li> <li>• Certifié ICP-Brasil</li> </ul>	<ul style="list-style-type: none"> <li>• CC EAL 5 + (puce)</li> <li>• Conforme CE, FCC, RoHS</li> </ul>

## SDK PKI

Notre kit de développement logiciel PKI inclut tout ce dont vous avez besoin pour l'intégration de la PKI à votre logiciel. Le kit comprend des bibliothèques, des exemples de code et une documentation détaillée pour C, C++ et Java.