EVIDEN

CardOS Security Token

FIDO2 et PKI avec la clé USB

Aperçu

Avec le CardOS Security Token, Eviden propose une solution de token USB pour les applications PKI et FIDO2, comprenant une puce cryptographique pour les fonctions de sécurité, les opérations cryptographiques, et la création et le stockage sécurisés de clés cryptographiques et de certificats.

CardOS met en valeur la grande expertise d'Eviden en tant que leader européen de l'intégration de systèmes et du développement de cartes à puce.

Basé sur CardOS USB V5.6, le jeton de sécurité CardOS inclut une interface de communication sans contact en plus de l'interface USB. Cette solution s'intègre parfaitement dans les environnements informatiques avec des mobiles, des tablettes et des ordinateurs portables qui ne disposent pas d'un lecteur de carte à puce interne.

Points forts

CardOS Security Token – PKI

Basés sur l'infrastructure à clé publique (PKI), les clés et certificats cryptographiques sont essentiels pour sécuriser les activités en ligne d'aujourd'hui. L'ICP est utilisée pour sécuriser le courrier électronique, les signatures numériques, l'authentification des services et la connexion aux postes de travail.

Le dispositif de sécurité CardOS permet de créer, de stocker et d'utiliser en toute sécurité des clés et des certificats pour effectuer toutes les opérations de sécurité nécessaires.

Associé à un intergiciel ("middleware") pour carte à puce disponible séparément (CardOS API, SCinterface), CardOS Security Token offre une solution idéale et facile à utiliser pour sécuriser les applications standard. Le logiciel intermédiaire pour cartes à puce, avec ses interfaces standard, permet une intégration et une utilisation transparentes des clés et des certificats stockés dans des applications standard sous Windows, Linux et macOS.

Dispositifde sécurité CardOS - FIDO2

Les mots de passe sont souvent jugés inadéquats et sont considérés comme le maillon faible de l'authentification par les experts en sécurité, car ils peuvent être compromis plus facilement que d'autres méthodes. La création de mots de passe forts et uniques pour chaque compte devient rapidement un défi pour les utilisateurs. Le rapport 2021 Verizon Data Breach Investigation Report[1] indique que 61 % des violations impliquent des informations d'identification, dont 25 % à partir d'informations d'identification volées.

[1] www.verizon.com/business/resources/reports/dbir/

Eviden propose FIDO2 pour répondre à ces défis, permettant aux utilisateurs de se connecter à leurs applications et services avec une sécurité beaucoup plus élevée. Cela permet aux organisations de mettre en œuvre une authentification à deux facteurs avec FIDO2, combinant quelque chose que vous avez (le token) avec quelque chose que vous connaissez (le PIN secret du token) pour une authentification sécurisée.

Le jeton de sécurité CardOS offre l'avantage d'utiliser un seul authentificateur pour plusieurs connexions à différentes applications, ne nécessitant qu'un seul code PIN pour permettre l'accès à l'authentificateur. Le jeton de sécurité CardOS est conçu pour les clients du marché public ou des entreprises. L'authentification sécurisée et pratique sans mot de passe est une tendance croissante, et de nombreux services offrent déjà la possibilité d'utiliser l'authentification FIDO2.

Plate-forme matérielle et système d'exploitation

CardOS USB V5.6, le système d'exploitation de la carte à puce utilisé dans le jeton de sécurité CardOS, est basé sur la technologie de sécurité numérique innovante « Integrity Guard » d'Infineon et est implémentée sur la plateforme de contrôleur de sécurité SLE78. La puce utilisée est le SLE78CLUFX5000PHM, avec laquelle environ 160 kB de mémoire utilisateur sont disponibles.

CardOS USB V5.6 est un système d'exploitation natif multifonctionnel pour cartes à puce, extensible par des paquets personnalisés pour améliorer ou modifier ses fonctionnalités. Il offre des algorithmes cryptographiques de pointe, notamment AES, SHA-2 et les courbes elliptiques.

Qu'est-ce que FIDO2[2]?

FIDO2 (Fast IDentity Online) offre une méthode d'authentification sûre, pratique et simple. Les spécifications de FIDO2 visent à éliminer les risques de vol de mot de passe et d'attaques par hameçonnage.

L'utilisateur s'inscrit à une application ou un service web

Son enregistrement génère une clé publique et une clé privée

Lors de la demande d'accès au service web, un défi est généré

Le défi est signé avec les données clés du service web et renvoyé.

L'utilisateur peut se connecter avec succès

Token de sécurité CardOS comme authentificateur FIDO2

Avec le jeton de sécurité CardOS, Eviden propose un authentificateur FIDO2 basé sur le système d'exploitation CardOS USB V5.6, conforme aux spécifications FIDO2 et certifié par l'Alliance FIDO™.

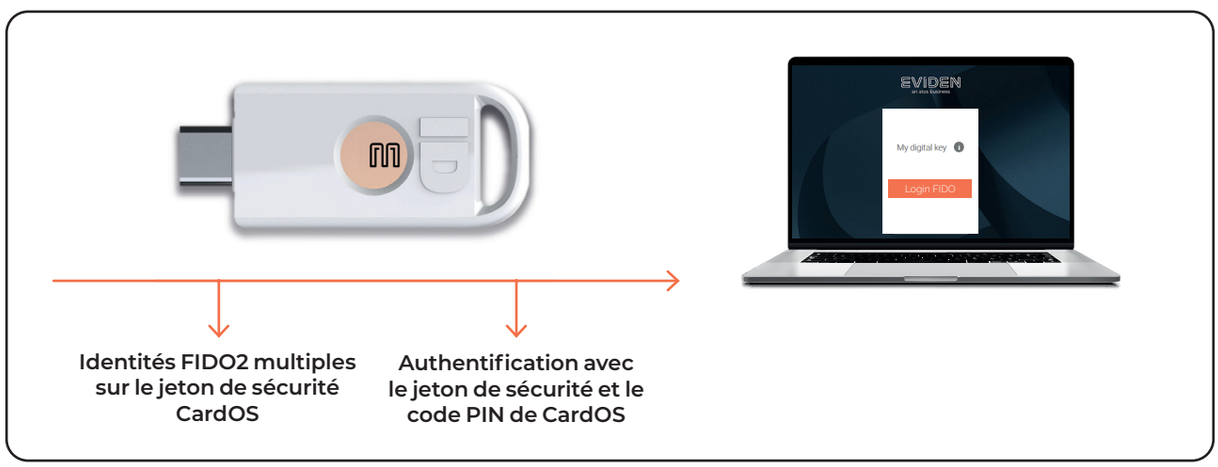
L'authentification FIDO2 repose sur la cryptographie à clé publique. En s'appuyant sur les mécanismes de sécurité robustes de CardOS, les clés utilisées pour l'authentification sont créées à l'intérieur du système. clés utilisées pour l'authentification sont créées dans la puce CardOS et ne la quittent jamais.

Prenant en charge le protocole FIDO2/CTAP[3], le jeton de sécurité CardOS permet une authentification sans mot de passe pour les services acceptant ou exigeant l'authentification FIDO. acceptant ou exigeant l'authentification FIDO.

Le jeton de sécurité CardOS constitue une solution sûre et pratique pour l'authentification sans mot de passe. Les utilisateurs finaux n'ont qu'à s'authentifier avec leur token de sécurité CardOS et un code PIN, si le serveur l'exige, ce qui évite de devoir se souvenir de mots de passe et de noms de connexion, ce qui évite de devoir se souvenir de mots de passe et de noms de connexion. Cela permet également de réduire les coûts du service d'assistance liés à la réinitialisation des mots de passe.

[2] Les marques et logos FIDO, FIDO ALLIANCE, FIDO AUTHENTICATION, FIDO CERTIFIED et FIDO2 sont des marques commerciales de FIDO Alliance.

[3] Le protocole CTAP (Client To Authenticator Protocol) est une spécification permettant la communication entre un client et un authentificateur externe.



Jeton de sécurité CardOS pour une variété d'applications

Le jeton de sécurité CardOS est parfait pour les environnements informatiques et les appareils sans lecteur de carte à puce intégré, éliminant ainsi le besoin d'un lecteur de carte supplémentaire par rapport aux solutions basées sur les cartes à puce. Il prend en charge diverses options d'authentification, notamment la fonctionnalité PKI, OTP et FIDO, dans n'importe quelle combinaison

- **Token de sécurité CardOS comme authentificateur FIDO 2**
- **Token de sécurité CardOS comme authentificateur FIDO2 avec fonctionnalité PKI intégrée (PKCS#15, CardOS API /SCinterface)**
- **Jeton de sécurité CardOS comme authentificateur FIDO2 avec PKI et OTP (pour utilisation avec CardOS SmartOTP)**
- **Jeton de sécurité CardOS avec PKI et OTP en option**

Jeton de sécurité CardOS – Connectivité

Le jeton de sécurité CardOS offre deux options de connectivité : USB et l'interface sans contact intégrée. Cette dernière permet au token de se connecter à des appareils mobiles via leur interface NFC.

En outre, l'interface sans contact du jeton de sécurité CardOS prend en charge les solutions d'accès physique grâce à l'émulation classique MIFARE d'une puce MIFARE 4k.

Protocoles de communication

Protocols USB:

- CCID
  - pour une utilisation avec les pilotes de lecteur couramment installés sous Windows, Linux et macOS
  - pour une utilisation standard en entreprise avec un middleware de carte à puce, CardOS API / SCinterface avec des applications standard qui utilisent les interfaces Minidriver, PKCS#11 et CTK
- HID
  - la prise en charge de la spécification de l'authentificateur FIDO2.0/2.1

Protocole de transmission selon:

- T=CL (protocole ISO/IEC 14443-4 de type A)
- Prise en charge des APDU de longueur étendue conformément à la norme ISO/IEC 7816-4
- Communication par carte sans contact jusqu'à 848 kbauds
- Étiquette NFC de type 4

Outils et soutien

Pour faciliter l'intégration de CardOS, Eviden fournit à ses clients :

- Manuels et fichiers de script
- Outil de script pour l'exécution des commandes de cartes et le chargement des paquets Service professionnel : - Assistance professionnelle pour les projets d'intégration - Paquets et structures de fichiers personnalisés
- CardOS API ou SCinterface, le middleware d'interface cryptographique standard pour le token CardOS avec Microsoft Base CSP et PKCS#11.
- CardOS SmartOTP, l'application logicielle pour le calcul de l'OTP
- Fourniture de solutions complètes clés en main pour l'enregistrement, l'utilisation et la révocation des jetons de sécurité CardOS

Normes et points forts techniques

Interfaces de communication

- USB 2.0:
  - Connecteur USB de type A
  - Connecteur USB de type C
- NFC:
- T=CL (ISO14443/IEC 14443-4 Type A)

Certifications

- FIDO2 Niveau 1

Systèmes d'exploitation pris en charge*

- Windows 10, 11
- Linux
- macOS
- Android
- iOS

* Toutes les applications peuvent ne pas être prises en charge

Dimensions

- USB Type A: 52 x 20 x 5 mm
- USB Type C: 50 x 20 x 6 mm

Plage de température

- Plage de température de fonctionnement : 0°C à +40°C
- Plage de température de stockage : -20°C à +85°C

Connect with us

/in/eviden
@EvidenLive
@evidenlive
/EvidenLive

eviden.com