

Dispositifs SafeNet FIDO2

Donnez à votre entreprise la capacité de mettre en place une authentification sans mot de passe forte et sécurisée



A l'aube de la décennie 2020, alors que les entreprises poursuivent leur transformation numérique et adoptent le cloud, la majorité des failles de sécurité est liée au vol d'identités. De nombreuses organisations ont investi dans des programmes d'authentification forte, dont l'authentification basée sur la PKI.

Ces organisations doivent désormais faire face à de nouveaux cas d'usage, tout en conservant un équilibre optimal entre sécurité et simplicité d'utilisation.

Comment les organisations créent-elles une expérience de connexion simple sans mot de passe sur tous les appareils ? Comment les entreprises peuvent-elles répondre à ces nouveaux cas d'usage sans remplacer l'ensemble de leurs méthodes d'authentification ? Thales, le leader mondial de la sécurité numérique, répond à ces questions avec deux nouveaux dispositifs SafeNet FIDO2 : la carte intelligente SafeNet IDPrime 3940 FIDO et le token USB SafeNet eToken FIDO. Ces nouvelles solutions permettent aux organisations de sécuriser l'adoption du cloud et de sécuriser les accès dans des environnements hybrides grâce à une offre d'authentification et de gestion des accès intégrée.

Authentification sans mot de passe

L'authentification sans mot de passe remplace les mots de passe par d'autres méthodes d'identification, améliorant ainsi les niveaux d'assurance et de confort. Ce type d'authentification a gagné du terrain en raison de sa capacité à faciliter considérablement l'expérience de connexion pour les utilisateurs et à remédier aux vulnérabilités inhérentes aux mots de passe textuels. Ces avantages comprennent une réduction de la friction, un niveau de sécurité plus élevé offert pour chaque appli et l'élimination des anciens mots de passe.

Confort pour les clients PKI

L'un des plus gros avantages de cette offre est que les entreprises qui s'appuient sur l'authentification par PKI peuvent désormais utiliser une carte intelligente combinée PKI-FIDO pour faciliter leurs initiatives de transformation numérique et cloud en permettant à leurs utilisateurs de n'utiliser qu'un seul appareil d'authentification pour sécuriser leur accès aux anciens domaines réseau, applis et services du cloud.

Support FIDO2 et PKI, appareil tout en un

La smartcard SafeNet IDPrime 3940 FIDO est conçue pour fonctionner avec les applications basées sur la PKI et elle est livrée avec un minidriver SafeNet qui offre une intégration parfaite avec le support natif des environnements Microsoft®, sans qu'il n'y ait besoin d'intermédiaire.

Cette smartcard à interface double qui permet la communication soit via une interface de contact, soit via une interface sans contact ISO 14443, est également compatible avec certains lecteurs NFC.

La carte SafeNet IDPrime 3940 FIDO est certifiée CC EAL5+/PP Java Card pour la plateforme Java et CC EAL5+/PP QSCD pour la combinaison de la plateforme Java et de l'applet PKI. SafeNet IDPrime 3940 est qualifiée par l'ANSSI et selon les réglementations eIDAS pour les applications eSignature et eSeal. En outre, SafeNet IDPrime 3940 FIDO respecte les normes FIDO 2.0 et U2F.

Token USB avec options Touch Sense

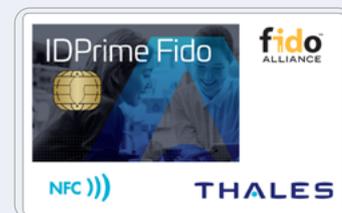
Le SafeNet eToken FIDO est un token USB, ce qui en fait la solution idéale pour les entreprises qui cherchent à déployer l'authentification sans mot de passe pour leurs employés. Cet authentificateur est un dispositif USB compact avec témoin d'intégrité et détecteur de présence qui crée un troisième facteur d'authentification : quelque chose que l'on possède (token physique), quelque chose que l'on connaît (code PIN), quelque chose que l'on fait (toucher le token).

Avantages clés

Les dispositifs SafeNet FIDO2 permettent à votre entreprise de mettre en place une authentification forte sans mot de passe pour n'importe quel environnement.

Ses avantages clés incluent :

- sécurisation de l'adoption du cloud et des accès dans des environnements hybrides grâce à une carte intelligente combinée PKI/FIDO
- accès sécurisé et facilité sur divers systèmes d'exploitation
- accès sans mot de passe aux applis cloud et domaines réseau
- optimisez votre programme d'authentification PKI sans le remplacer !
- offrez à vos utilisateurs un authentificateur unique pour tous leurs besoins
- certification CC
- support de tous les appareils et systèmes d'exploitation (sans intermédiaire)
- entièrement personnalisable
- parfait pour les signatures numériques et le chiffrement des e-mails



Caractéristiques du produit

Smartcard SafeNet IDPrime 3940 FIDO

Mémoire	<ul style="list-style-type: none"> • La SafeNet IDPrime 3940 est basée sur une puce mémoire 400 KB Java Flash. Une carte SafeNet IDPrime 3940 FIDO standard est livrée avec 20 conteneurs de clés. • La mémoire disponible pour les certificats et d'autres applets et données dans cette configuration standard est de 63 KB.
Normes	<ul style="list-style-type: none"> • Minidriver BaseCSP (minidriver SafeNet) • Global Platform 2.2.1 • Java Card 3.0.4 • ISO 7816 et ISO 14443 • Certifications FIDO 2.0 et U2F
Systèmes d'exploitation	<ul style="list-style-type: none"> • Application FIDO supportée par Windows 10 et les autres systèmes d'exploitation compatibles avec FIDO. • Application PKI standard supportée par Windows, MAC OS X et Linux
Algorithmes cryptographiques	<ul style="list-style-type: none"> • Hash : SHA-1, SHA-256, SHA-384, SHA-512 • RSA : jusqu'à RSA 4 096 bits • RSA OAEP & RSA PSS • ECDSA et ECDH P-256 bits. ECDSA et ECDH P-384 et P-521 bits disponibles via une configuration personnalisée • Génération de paires de clés asymétriques sur carte (RSA jusqu'à 4096 bits et courbes elliptiques jusqu'à 521 bits) • Symétrique : AES pour sécuriser la messagerie et 3DES pour Microsoft Challenge/Response uniquement
Protocoles de communication	<ul style="list-style-type: none"> • T=1, T=0, PPS, avec un taux de baud pouvant atteindre 446 Kbps à 3,57 MZ (TA1=97 h) • T=CL, ISO 14443 type A, avec une vitesse pouvant atteindre 848 Kbps
Autres fonctionnalités	<ul style="list-style-type: none"> • Paramètres du PIN intégré • Support PIN multiple • La famille de cartes SafeNet IDPrime peut être personnalisée (corps et programme de la carte) pour répondre aux besoins du client.

Caractéristiques de la puce

Technologie	<ul style="list-style-type: none"> • Moteur cryptographique intégré pour un chiffrement symétrique et asymétrique
Durée de vie	<ul style="list-style-type: none"> • Minimum de 500 000 cycles d'écriture/suppression • Conservation des données pour au moins 25 ans
Certificat	<ul style="list-style-type: none"> • CC EAL6+
Sécurité	<ul style="list-style-type: none"> • Les cartes SafeNet IDPrime disposent de nombreuses contremesures matérielles et logicielles pour se protéger des attaques, dont les attaques par canal auxiliaire, les attaques invasives et les attaques par faute. • La SafeNet IDPrime 3940 FIDO est certifiée CC EAL5+/PP Java Card pour la plateforme Java et CC EAL5+/PP QSCD pour la combinaison de la plateforme Java et de l'applet PKI. Elle est également qualifiée eIDAS pour l'eSignature et l'eSeal et qualifiée par l'ANSSI.

Caractéristiques du produit

SafeNet eToken FIDO



Mémoire

- 90 K

Standards

- FIDO 2.0 et FIDO U2F

Systèmes d'exploitation

- Application FIDO supportée par Windows 10 et les autres systèmes d'exploitation compatibles avec FIDO.

Dimensions

Physiques

- 6 mm x 8 mm x 40,5 mm

Température de fonctionnement

- de 0 ° C à 70 ° C

Température de stockage

- de -40 ° C à 85 ° C

Taux d'humidité

- 0-100 % sans condensation

Certificat d'étanchéité

- IP X7 – IEC 529 -

Connectique USB

- USB type A ; supporte USB 1.1 et 2.0 (pleine vitesse)

Boîtier

- Plastique dur moulé, témoin d'intégrité

Mémoire de conservation des données

- Au moins 10 ans

Réécritures de la mémoire

- Au moins 500 000

SafeNet IDPrime 3940 FIDO/SafeNet eToken FIDO est compatible avec les comptes Microsoft Azure Active Directory.

À propos des solutions SafeNet d'Access Management et d'authentification de Thales

Les solutions d'authentification et de gestion des accès de Thales permettent aux entreprises de gérer de manière centralisée et sécurisée les accès à leurs réseaux informatiques et à leurs applis web et cloud. Grâce au SSO basé sur des règles d'accès et aux méthodes d'authentification universelles, les entreprises peuvent efficacement prévenir les brèches, migrer vers le cloud sans danger et faciliter la mise en conformité réglementaire.

À propos de Thales

Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.