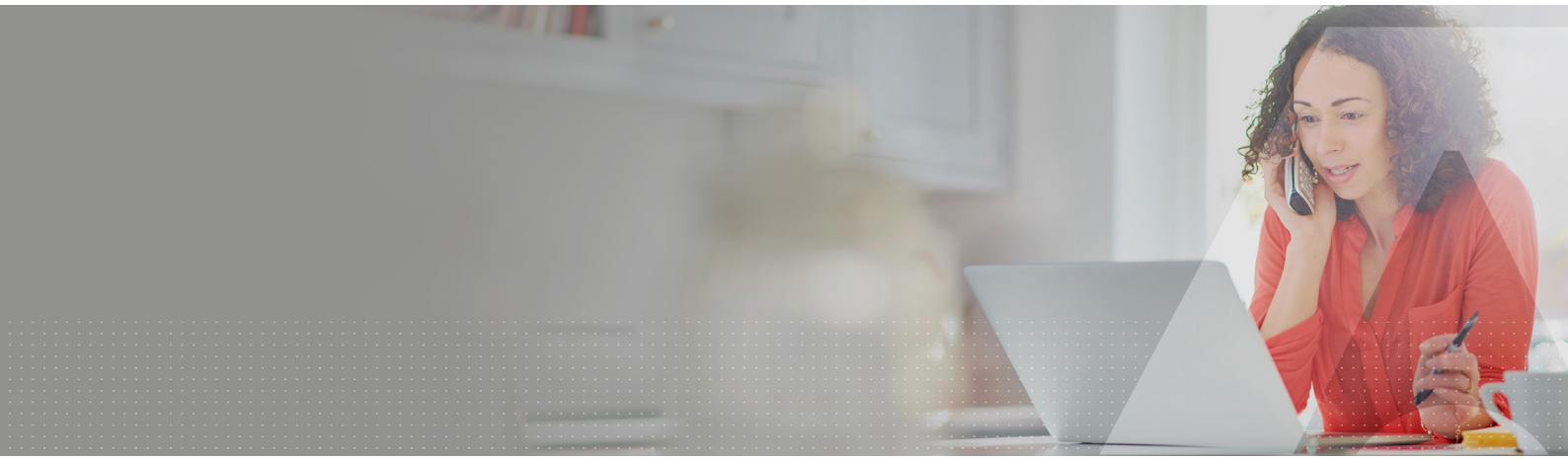
cpl.thalesgroup.com

THALES
Building a future we can all trust

Dispositifs SafeNet FIDO2 sans mot de passe

Réduisez le risque des failles de sécurité avec l'authentification multi-facteurs sans mot de passe



Les organisations qui sont en plein processus de transformation numérique déplacent des applications et des données vers le cloud pour (1) favoriser l'accessibilité de n'importe où et (2) réduire les coûts opérationnels. Les utilisateurs se connectant à un nombre grandissant d'applications cloud, les mots de passe faibles deviennent la première cause de vol d'identité et de brèches de sécurité.

Pour réduire les risques associés à votre ouverture de session Windows, à vos applications SaaS, à vos utilisateurs dotés de privilèges élevés et à vos utilisateurs en général, Thales prend en charge l'authentification FIDO sans mot de passe à l'aide de dispositifs matériels d'authentification multi-facteurs (MFA).

Remplacer les mots de passe par du matériel d'authentification FIDO introduit une expérience d'authentification multi-facteurs sans mot de passe moderne qui résiste aux attaques d'hameçonnage et aux usurpations de comptes, et qui permet de garantir la conformité.

Les dispositifs d'authentification multi-facteurs utilisent des protocoles actuels et émergents pour prendre en charge plusieurs applications en même temps. Utilisez une clé qui combine la prise en charge de FIDO2, WebAuthn, U2F, et PKI pour accéder aux espaces physiques et aux ressources logiques.

Authentification FIDO2 sans mot de passe

L'authentification FIDO sans mot de passe réduit le risque de brèches de sécurité en remplaçant les mots de passe textuels vulnérables par une authentification FIDO.

L'authentification FIDO a gagné du terrain en tant que forme d'authentification multi-facteurs moderne 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. Les avantages incluent notamment une réduction de la friction pour les utilisateurs et un haut niveau de sécurité.

Autorisez plusieurs méthodes d'authentification utilisateur

Thales, le leader mondial dans le domaine de la sécurité numérique, prend en charge plusieurs méthodes d'authentification sans mot de passe avec une gamme puissante de dispositifs FIDO.

FIDO avec badge convergé

Accès physique : pour un confort optimal, les cartes à puce FIDO de Thales prennent en charge l'accès physique permettant aux utilisateurs d'accéder aux espaces physiques et aux ressources logiques avec une seule carte à puce personnalisable.

Étendre l'authentification moderne aux environnements PKI : les organisations qui s'appuient sur l'authentification par PKI peuvent désormais utiliser une carte à puce 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, applications et services du cloud.

Accès à distance

Qu'ils travaillent de chez eux ou en déplacement, les utilisateurs peuvent se connecter aux applications cloud d'entreprise depuis plusieurs appareils, à plusieurs endroits.

Les dispositifs d'authentification FIDO fournissent un accès à distance sécurisé avec une authentification multi-facteurs pour protéger votre organisation, indépendamment de l'appareil de terminaison et de l'emplacement.

PC Windows et connexion réseau

Les dispositifs d'authentification FIDO fournissent une authentification multi-facteurs sans mot de passe, permettant aux utilisateurs d'accéder aux PC et tablettes Windows. Avec les cartes PKI FIDO combinées, nous pouvons offrir un seul appareil pour une connexion sécurisée dans tous les systèmes d'exploitation, y compris Window 10, 8 et 7, Windows Server, macOS et Linux. Ainsi, les organisations peuvent utiliser les appareils PKI FIDO de Thales pour répondre aux besoins de FIDO en matière d'authentification PKI et de signature numérique.

Protéger les applications SaaS

Puisque la majorité des utilisateurs utilisent les mêmes mots de passe avec plusieurs applications, vous pouvez améliorer considérablement votre sécurité et réduire les demandes d'assistance en proposant des dispositifs d'authentification FIDO. Les dispositifs FIDO de Thales sont entièrement compatibles avec Azure AD et garantissent un accès sécurisé aux applications Azure AD gérées.

Accès mobile sécurisé

Les dispositifs FIDO de Thales permettent une authentification moderne sur tous les appareils en offrant aux utilisateurs une méthode d'authentification sans contact de type « Tap & go » afin d'obtenir un accès sécurisé à toutes les ressources cloud de n'importe quel appareil.

Gestion des accès privilégiés

Les utilisateurs privilégiés avec des autorisations élevées ou la possibilité de se connecter aux solutions PAM ont un accès en lecture aux données sensibles : leurs comptes sont la cible ultime des acteurs malveillants.

Le fait de fournir aux utilisateurs privilégiés une authentification multi-facteurs pour remplacer les mots de passe vulnérables garantit que seuls les utilisateurs autorisés peuvent accéder aux ressources privilégiées.

Compatibilité IDP

Les dispositifs sans mot de passe SafeNet FIDO2 sont compatibles avec tous les fournisseurs d'identité (IDP) qui prennent en charge la norme FIDO2.

Consultez notre site Internet pour une liste des IDP avec lesquels nous avons effectué nos tests et que nous avons validés : htthttps://cpl.thalesgroup.com/access-management/authenticators/fido-devices

Pour toutes les entreprises, offrez à vos employés et vos sous-traitants un seul dispositif pour tous leurs besoins en matière d'authentification et d'accès, qu'ils travaillent de chez eux ou au bureau. Facilitez l'accès physique aux bâtiments et aux zones contrôlées et la mobilité des employés. Étudiez vos cas d'utilisation et choisissez vos dispositifs d'authentification SafeNet FIDO.

Caractéristiques du produit	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Facteur de forme	Carte à puce	Token USB-A	Carte à puce	Carte à puce	Carte à puce
Contact (ISO 7816)	FIDO et PKI	S/O	S/O	PKI	PKI
Sans-contact (ISO144443)	FIDO et PKI	S/O	FIDO et accès physique	FIDO et accès physique	FIDO et accès physique
Mémoire					
Puce mémoire	Java Flash 400 KB	Java Flash 400 KB	ROM utilisateur 586 KB	Puce de contact : Java Flash 400 KB Puce sans contact : ROM utilisateur 586 KB	Puce de contact : Java Flash 400 KB Puce sans contact : ROM utilisateur 586 KB
Mémoire libre disponible pour les clés résidentes, les certificats et les applets et données supplémentaires	73 KB	90 KB	88,3 – 98,3 KB	Contact : 73 KB Sans contact : 88,3 – 98,3 KB	Contact : 73 KB Sans contact : 88,3 – 98,3 KB
Capacité des clés					
Clés FIDO résidentes	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8
Conteneurs de clés PKI	20	S/O	S/O	20	20
Normes prises en charge					
Carte Java	3.0.4	3.0.4	S/O	3.0.4	3.0.5
Global Platform 2.2.1	✔	✔	S/O	✔	✔
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Minidriver Base CSP (minidriver SafeNet)	✔	S/O	S/O	✔	✔
Algorithmes cryptographiques (PKI)					
Hash : SHA-1, SHA-256, SHA-384, SHA-512.	✔	S/O	S/O	✔	✔
RSA : jusqu'au RSA 4 096 bits	✔	S/O	S/O	✔	✔
RSA OAEP et RSA PSS	✔	S/O	S/O	✔	✔
ECDSA et ECDH P-256 bits. ECDSA et ECDH P-384 et P-521 bits disponibles via une configuration personnalisée	✔	S/O	S/O	✔	✔
Génération de paires de clés asymétriques sur carte (RSA jusqu'à 4 096 bits et courbes elliptiques jusqu'à 521 bits)	✔	S/O	S/O	✔	✔
Symétrique : AES pour sécuriser la messagerie et 3DES pour Microsoft Challenge/Response uniquement	✔	S/O	S/O	✔	✔

Caractéristiques du produit	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certificats					
Chip : CC EAL6+	✔	✔	S/O	✔	✔
Certification NIST - FIPS 140-2, niveau 2	S/O	S/O	S/O	S/O	✔
Plateforme Java : certifiée CC EAL5+/PP Java Card	✔	✔	S/O	✔	S/O
Plateforme Java + applet PKI : CC EAL5+/PP QSCD	✔	S/O	S/O	✔	S/O
eIDAS qualifié pour eSignature et eSeal	✔	S/O	S/O	✔	S/O
ANSSI (France)	✔	S/O	S/O	✔	S/O
Accès physique : configurations Mifare Classic et DesFire	S/O	S/O	✔	✔	✔
Autres fonctionnalités					
Paramètres du PIN intégré	✔	S/O	S/O	✔	✔
Support PIN multiple	✔	S/O	S/O	✔	✔
Personnalisation et stratégie de marque	✔	S/O	S/O	✔	✔
Systèmes d'exploitation					
FIDO supporté par Windows 10 et les autres systèmes d'exploitation compatibles avec FIDO	✔	✔	✔	✔	✔
PKI prise en charge dans Windows, macOS X et Linux	✔	S/O	S/O	✔	✔

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.

> cpl.thalesgroup.com/fr <

Nous contacter – Pour consulter les emplacements de tous nos bureaux et nos coordonnées, veuillez vous rendre à la page cpl.thalesgroup.com/fr/contact-us