cpl.thalesgroup.com

THALES
Building a future we can all trust

Dispositifs FIDO2 de Thales :

Stoppez les attaques par hameçonnage grâce à l'authentification multifacteur forte sans mot de passe

Les organisations en processus de transformation numérique migrent des applications et des données vers le cloud pour favoriser leur accessibilité et réduire les coûts opérationnels. Les utilisateurs se connectant à un nombre grandissant d'applications cloud, les mots de passe, vulnérables, deviennent la première cause de vol d'identité et de violations de sécurité.

Répondant à ce risque, les dispositifs FIDO2 de Thales offrent aux organisations une authentification sans mot de passe résistante aux attaques par hameçonnage, ce qui leur permet de se protéger contre l'usurpation de comptes et d'éliminer les risques d'accès non autorisés aux ressources sensibles telles que les applications SaaS et les terminaux Windows.

Les dispositifs FIDO2 de Thales sont multi-applicatifs. Utilisez-en un qui combine FIDO2, U2F, PKI et RFID pour accéder aux espaces physiques et aux ressources logiques.

Authentification FIDO2 sans mot de passe

L'authentification FIDO2 élimine le risque d'usurpation de comptes en remplaçant les mots de passe vulnérables par un identifiant WebAuthn résistant aux attaques par hameçonnage.

L'authentification FIDO2 a gagné du terrain en tant que forme d'authentification multifacteur moderne en raison de sa capacité à faciliter l'expérience utilisateur lors de la connexion et à remédier aux vulnérabilités inhérentes aux mots de passe. Les avantages incluent notamment une réduction de la friction pour les utilisateurs et un haut niveau de protection contre les attaques par hameçonnage.

Respectez les mandats de conformité stricts

Grâce aux clefs de sécurité FIDO2 de Thales, tokens USB et cartes à puce, vous pouvez respecter toutes vos exigences règlementaires. Ils sont certifiés FIDO2 et U2F. Les dispositifs combinés PKI-FIDO sont conformes aux réglementations NIST, sont certifiés FIPS 140-2 ou Critères Communs (CC) et qualifiés ANSSI pour la plateforme Java et l'applet PKI. Ils respectent également les réglementations eIDAS pour les applications eSignature et eSeal.

Activez pour vos utilisateurs de multiples parcours d'authentification

Thales prend en charge de nombreux parcours d'authentification sans mot de passe avec une large gamme d'appareils FIDO.

Sécurisez l'accès aux 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 appels au support en équipant vos utilisateurs d'authentificateurs FIDO.

Connexion réseau pour les travailleurs de première ligne

Les clés de sécurité FIDO2 fournissent une authentification multi-facteur sans mot de passe qui permet aux utilisateurs, comme les travailleurs de première ligne, d'ouvrir une session en toute sécurité sur des postes partagés tels que des PC et des tablettes Windows.

Combinez accès physique et accès logique

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.

Modernisez les environnements PKI/CBA

Les organisations déjà équippées d'une infrastructure PKI et d'authentification basée sur les certificats peuvent désormais utiliser une carte à puce ou un token USB combiné PKI-FIDO pour faciliter leurs initiatives de transformation cloud et numérique. En fournissant à leurs utilisateurs un seul dispositif d'authentification pour sécuriser l'accès aux applications historiques, aux domaines réseau et aux services cloud, elles réduisent les coûts d'exploitation et simplifient l'expérience utilisateur.

Accès à distance sécurisé

Qu'ils travaillent de chez eux ou en déplacement, les utilisateurs peuvent se connecter aux applications Web depuis plusieurs appareils, à plusieurs endroits. Les clés de sécurité FIDO fournissent un accès à distance sécurisé avec une authentification multifacteur pour protéger votre organisation, indépendamment du terminal et de l'emplacement.

Accès mobile sécurisé

Les dispositifs FIDO de Thales permettent aux utilisateurs de s'authentifier sur n'importe quelle ressource cloud depuis leur appareil mobile : soit en posant leur carte à puce sur leur appareil grâce à la technologie NFC, soit en branchant le token USB-C SafeNet eToken Fusion à leur téléphone mobile.

Contrôle d'accès d'utilisateur privilégié

Les utilisateurs privilégiés disposant de permissions élevées (administrateurs, VIP, etc.) ont facilement accès aux données sensibles : leurs comptes constituent donc une cible choix pour les attaques par hameçonnage ciblé.

Le fait de fournir aux utilisateurs privilégiés des clés de sécurité FIDO2 pour remplacer les mots de passe vulnérables garantit que seuls les utilisateurs autorisés peuvent accéder aux ressources privilégiées.

Compatibilité IDP

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

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

Plateformes prises en charge

Les clés de sécurité PKI/FIDO de Thales prennent en charge une vaste gamme de systèmes d'exploitation, comme iOS, Android, Windows 11, 10 et 8, Windows Server, macOS et Linux, notamment SafeNet Trusted Access et Microsoft Azure Active Directory.

Avantages des clés FIDO2 Thales

Une sécurité de pointe

- Thales contrôle l'intégralité du cycle de fabrication et développe ses propres bibliothèques cryptographiques FIDO, réduisant les risques de données compromises.

Prise en charge de plusieurs cas d'utilisation

- Combinez FIDO, PKI et l'accès physique avec un seul dispositif
- Bénéficiez d'une authentification robuste pour les terminaux mobiles

Conforme aux normes de sécurité élevées

- Certifié U2F et FIDO2
- Conforme aux réglementations américaines et européennes en matière d'authentification résistante aux attaques par hameçonnage
- Certifié FIPS et CC pour les opérations PKI

Robustesse et évolutivité, pour une durée de vie étendue

- Clés USB FIDO inviolables, en plastique dur moulé
- Pas de dommage aux ports USB grâce à un capteur de détection de présence très sensible
- Prise en charge des mises à jour de micrologiciel pour une maintenance et une évolutivité améliorées

Caractéristiques du produit	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Avec contact (ISO 7816)	FIDO et PKI	FIDO et PKI	S/O	PKI	PKI
Sans contact (ISO 14443)	FIDO et PKI	FIDO et PKI	FIDO et accès physique	FIDO et accès physique	FIDO et accès physique
Mémoire					
Puce mémoire	Java Flash 400 Ko	Java Flash 400 Ko	ROM utilisateur 586 Ko	Puce avec contact : Java Flash 400 Ko Puce sans contact : ROM utilisateur 586 Ko	Puce avec contact : Java Flash 400 Ko Puce sans contact : ROM utilisateur 586 Ko
Mémoire libre disponible pour les clés résidentes, les certificats et les applets et données supplémentaires	73 Ko	55 Ko	88,3 – 98,3 Ko	Avec contact : 73 Ko Sans contact : 88,3 – 98,3 Ko	Avec contact : 73 Ko Sans contact : 88,3 – 98,3 Ko
Capacité de clés					
Clés FIDO résidentes	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8
Conteneurs de clés PKI	20	20	S/O	20	20
Normes prises en charge					
Java Card	3.0.4	3.0.5	3.0.4	3.0.4	Puce avec contact : 3.0.5 Puce sans contact : 3.0.4
GlobalPlatform	2.2.1	2.2.1	2.3	Puce avec contact : 2.2.1 Puce sans contact : 2.3	Puce avec contact : 2.2. Puce sans contact : 2.3
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Minidriver Base CSP (minidriver SafeNet)	✔	✔	S/O	✔	✔
Algorithmes cryptographiques (PKI)					
Hash : SHA-1, SHA-256, SHA-384, SHA-512.	✔	✔	S/O	✔	✔
RSA : jusqu'au RSA 4 096 bits	✔	✔	S/O	✔	✔
RSA OAEP et RSA PSS	✔	✔	S/O	✔	✔
ECDSA et ECDH P-256 bits. ECDSA P-384 et P-521 bits,	✔	✔	S/O	✔	✔
Les dispositifs ECDH sont disponibles via une	✔	✔	S/O	✔	✔
configuration personnalisée	✔	✔	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	✔	✔
Symétrique : AES pour sécuriser la messagerie et 3DES pour authentification par défi-réponse sur Microsoft uniquement	✔	✔	S/O	✔	✔

Caractéristiques du produit	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certifications					
Puce : CC EAL6+	✔	✔	✔	✔	✔
Certification NIST – FIPS 140-2, niveau 2	S/O	✔	S/O	S/O	✔
Plateforme Java : certifiée CC EAL5+/PP Java Card	✔	S/O	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 PKI					
Paramétrage PIN intégré	✔	✔	S/O	✔	✔
Prise en charge PIN multiples	✔	✔	S/O	✔	✔
Personnalisation et apposition de logo	✔	✔	S/O	✔	✔
Certifications					
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	✔	✔

Token : facteur de forme

Caractéristiques du produit	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion certifié Critères Communs (CC)
Facteur de forme	USB-A	USB-A ou USB-C	USB-A ou USB-C
Mémoire			
Puce mémoire	Java Flash 400 Ko	Java Flash 400 Ko	Java Flash 400 Ko
Mémoire libre disponible pour les clés résidentes, les certificats et les applets et données supplémentaires	90 Ko	55 Ko	73 Ko
Capacité de clés			
Clés FIDO résidentes	Jusqu'à 8	Jusqu'à 8	Jusqu'à 8
Conteneurs de clés PKI	S/O	20	20
Normes prises en charge			
Java Card	3.0.4	3.0.4	3.0.4
GlobalPlatform	2.2.1	2.2.1	2.2.1
FIDO 2.0	✔	✔	✔
U2F	✔	✔	✔
Minidriver Base CSP (minidriver SafeNet)	S/O	✔	✔
Algorithmes cryptographiques (PKI)			
Hash : SHA-1, SHA-256, SHA-384, SHA-512.	S/O	✔	✔
RSA : jusqu'au RSA 4 096 bits	S/O	✔	✔
RSA OAEP et RSA PSS	S/O	✔	✔
ECDSA et ECDH P-256 bits. ECDSA P-384 et P-521 bits,	S/O	✔	✔
Les dispositifs ECDH sont disponibles via une	S/O	✔	✔
configuration personnalisée	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	✔	✔
Symétrique : AES pour sécuriser la messagerie et 3DES pour authentification par défi-réponse sur Microsoft uniquement	S/O	✔	✔

Caractéristiques du produit	 SafeNet eToken FIDO	 SafeNet eToken Fusion USB-A ou USB-C	 SafeNet eToken Fusion rtifié Critères Communs (CC)
Certifications			
Puce : CC EAL6+	✔	S/O	✔
Certification NIST – FIPS 140-2, niveau 2	S/O	S/O	S/O
Plateforme Java : certifiée CC EAL5+/PP Java Card	✔	S/O	✔
Plateforme Java + applet PKI : CC EAL5+/PP QSCD	S/O	S/O	✔
eIDAS qualifié pour eSignature et eSeal	S/O	S/O	✔
ANSSI (France)	S/O	S/O	✔
Accès physique : configurations Mifare Classic et DesFire	S/O	S/O	S/O
Autres fonctionnalités PKI			
Paramétrage PIN intégré	S/O	✔	✔
Prise en charge PIN multiples	S/O	✔	✔
Personnalisation et apposition de logo	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	✔	✔

À propos des solutions de gestion des identités et des accès OneWelcome de Thales

Les solutions de pointe de Thales en matière de gestion des identités et des accès pour les employés et les clients (CIAM) permettent aux entreprises de gérer de manière centralisée et sécurisée les accès à leurs réseaux informatiques et à leurs applications Web et cloud. Grâce au SSO basé sur des règles d'accès et aux méthodes d'authentification universelles, les entreprises peuvent efficacement prévenir les violations de données, 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.