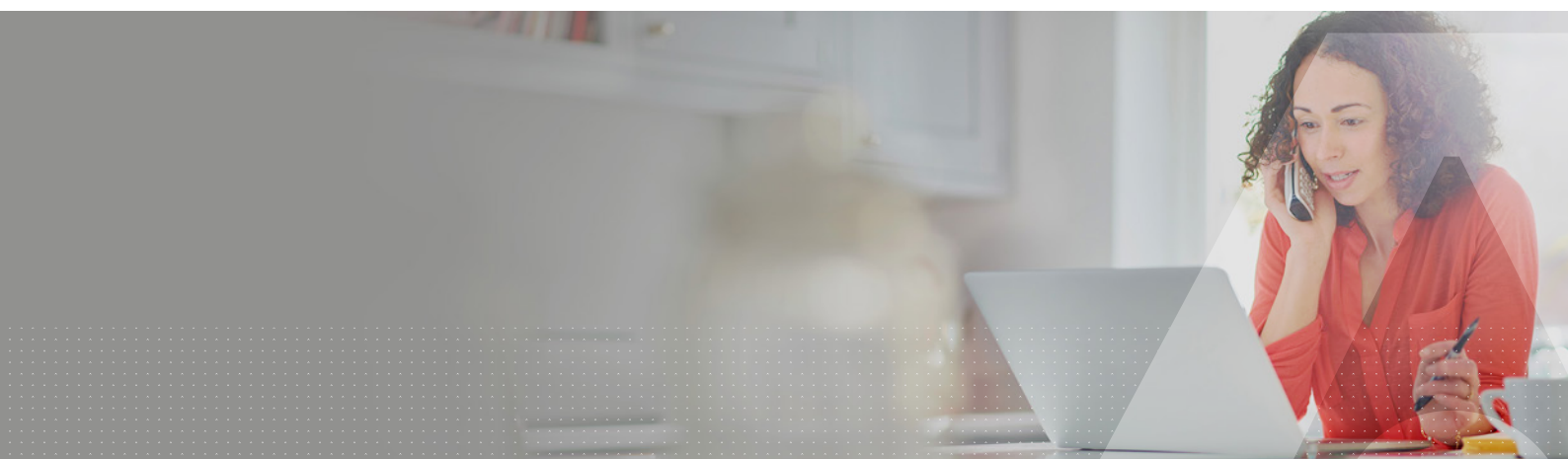


Dispozitive Passwordless (fără parolă) SafeNet FIDO2

Reduceți riscul de breșe de securitate cu Autentificarea multifactor Passwordless (fără parolă)



Organizațiile care își extind transformarea digitală își mută aplicațiile și datele în cloud pentru (1) a permite accesibilitatea de oriunde și (2) reduce costurile operaționale. Deoarece utilizatorii se autentifică într-un număr din ce în ce mai mare de aplicații bazate pe cloud, parolele slabe rezultă a fi principala cauză a furtului de identitate și a breșelor de securitate.

Pentru a reduce riscul la autentificarea în Windows și aplicațiile SaaS, a utilizatorilor cu privilegii înalte și a utilizatorilor în general, Thales susține autentificarea fără parolă FIDO, folosind dispozitive hardware de autentificare multifactor (MFA).

Înlocuirea parolelor cu hardware de autentificare FIDO introduce o experiență MFA fără parolă, modernă, care rezistă la atacurile de tip phishing și preluările de conturi, permițând totodată conformitatea.

Dispozitivele de autentificare multifactor Thales utilizează protocoalele actuale și nou apărute pentru a susține simultan mai multe aplicații. Utilizați o cheie care combină compatibilitatea cu FIDO2, WebAuthn, U2F și PKI pentru a accesa atât spațiile fizice, cât și resursele logice.

Autentificarea FIDO2 Passwordless (fără parolă)

Autentificarea FIDO fără parolă reduce riscul de breșe de securitate prin înlocuirea parolelor textuale, vulnerabile, cu autentificarea FIDO.

Autentificarea FIDO a devenit populară ca formă modernă de MFA, datorită beneficiilor sale considerabile în simplificarea experienței de autentificare pentru utilizatori și deoarece combate vulnerabilitățile inerente ale parolelor bazate pe text. Printre avantajele se numără complexitatea redusă pentru utilizatori și un nivel înalt de securitate.

Permiteți experiențe de autentificare multiple pentru utilizatori

Thales, liderul mondial în domeniul securității digitale, susține numeroase experiențe de autentificare fără parolă cu o gamă performantă de dispozitive FIDO



FIDO cu ecuson convergent

Acces fizic- Pentru comoditate optimă, cardurile inteligente Thales FIDO susțin accesul fizic, permițându-le utilizatorilor să acceseze atât spațiile fizice, cât și resursele logice cu un singur card inteligent și personalizabil.

Extindeți autentificarea modernă la mediile PKI -

Organizațiile care se bazează pe autentificarea PKI pot utiliza acum un card inteligent PKI-FIDO combinat pentru a facilita inițiativele lor de transformare digitală și trecere în cloud, furnizând utilizatorilor un singur dispozitiv de autentificare pentru securizarea accesului la aplicațiile vechi, domeniile de rețele și serviciile cloud.

Accesul la distanță

Fie că lucrează de acasă sau în timp ce călătoresc, utilizatorii se pot autentifica în aplicațiile de business bazate pe cloud, de pe dispozitive multiple și din locații multiple.

Dispozitivele de autentificare Thales FIDO oferă acces securizat, de la distanță și cu MFA, pentru a vă proteja organizația indiferent de dispozitivul de la punctul final și locație.

Autentificarea în PC-ul Windows și rețea

Dispozitivele de autentificare FIDO oferă MFA fără parolă, permițându-le utilizatorilor să acceseze în siguranță tabletele și PC-urile Windows. Cu cardurile FIDO PKI combinate, putem oferi un singur dispozitiv pentru autentificarea în siguranță în orice SO, inclusiv Windows 10, 8 și 7, Windows Server OS, macOS și Linux. Acest lucru înseamnă că organizațiile pot utiliza dispozitivele Thales FIDO-PKI pentru a susține atât autentificările FIDO și PKI, cât și necesitățile de semnătură digitală.

Protejați aplicațiile SaaS

Deoarece majoritatea utilizatorilor își refolosesc parolele pentru mai multe aplicații, puteți îmbunătăți semnificativ securitatea și reduce numărul de apeluri către Biroul de Asistență, echipând utilizatorii cu dispozitive de autentificare FIDO. Dispozitivele Thales FIDO sunt complet compatibile cu Azure AD și asigură accesul securizat la aplicațiile gestionate de Azure AD.

Acces mobil securizat

Dispozitivele Thales FIDO permit autentificarea modernă pe orice dispozitiv, lăsându-i utilizatorilor să se autentifice fără contact, pur și simplu „atinge și intră”, pentru a obține acces securizat la orice resursă cloud de pe orice dispozitiv mobil.

Gestionarea accesului privilegiat

Utilizatorii privilegiați cu permisiuni înalte sau cu posibilitatea de a se autentifica în soluții PAM au acces imediat la datele sensibile – conturile lor reprezintă ținta supremă a infractorilor cibernetici.

Oferindu-le utilizatorilor privilegiați autentificarea multifactor pentru a înlocui parolele vulnerabile, se asigură faptul că numai utilizatorii autorizați pot accesa resursele privilegiate.

Compatibilitatea IDP

Dispozitivele fără parolă SafeNet FIDO2 sunt compatibile cu orice furnizor de identitate (IDP) care acceptă standardul FIDO2.

Consultați site-ul nostru web pentru o listă a furnizorilor IDP pe care i-am testat și validat împreună: <https://cpl.thalesgroup.com/access-management/authenticators/fido-devices>

Pentru toate întreprinderile, oferiți-le angajaților și subcontractanților un singur dispozitiv pentru toate nevoile lor de autentificare și acces – fie că lucrează de acasă sau din birou. Permiteți accesul fizic în clădiri și zone controlate, facilitând totodată mobilitatea angajaților. Luați în calcul cazurile dvs. de utilizare și alegeți dintre dispozitivele de autentificare SafeNet FIDO.

Caracteristicile produselor	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Factor de formă	Card inteligent	Token USB-A	Card inteligent	Card inteligent	Card inteligent
Contact (ISO 7816)	FIDO și PKI	N/A	N/A	PKI	PKI
Fără contact (ISO14443)	FIDO și PKI	N/A	FIDO și acces fizic	FIDO și acces fizic	FIDO și acces fizic
Memorie					
Cip de memorie	400 kB Java Flash	400 kB Java Flash	586 kB User ROM	Cip cu contact: 400 kB Java Flash Cip fără contact: 586 kB User ROM	Cip cu contact: 400 kB Java Flash Cip fără contact: 586 kB User ROM
Memorie liberă disponibilă pentru chei rezidente, certificate, applet-uri și date suplimentare	73 kB	90 kB	88,3 – 98,3 kB	Contact: 73 kB Fără contact: 88,3 – 98,3 kB	Contact: 73 kB Fără contact: 88,3 – 98,3 kB
Capacitatea cheii					
Chei rezidente FIDO	Maxim 8	Maxim 8	Maxim 8	Maxim 8	Maxim 8
Containere de chei PKI	20	N/A	N/A	20	20
Standarde compatibile					
Java Card	3.0.4	3.0.4	N/A	3.0.4	3.0.5
Global Platform 2.2.1	✓	✓	N/A	✓	✓
FIDO 2.0	✓	✓	✓	✓	✓
U2F	✓	✓	✓	✓	✓
Minidriver Base CSP (minidriver SafeNet)	✓	N/A	N/A	✓	✓
Algoritmi criptografici (PKI)					
Combinare: SHA-1, SHA-256, SHA-384, SHA-512.	✓	N/A	N/A	✓	✓
RSA: până la RSA 4.096 biți	✓	N/A	N/A	✓	✓
RSA OAEP și RSA PSS	✓	N/A	N/A	✓	✓
P-256 biți ECDSA, ECDH. P-384 și P-521 biți ECDSA, ECDH sunt disponibile printr-o configurare personalizată	✓	N/A	N/A	✓	✓
Generare perechi de chei asimetrice pe card (RSA de până la 4.096 biți și curbe eliptice de până la 521 biți)	✓	N/A	N/A	✓	✓
Simetric: AES—Pentru mesagerie securizată și 3DES doar pentru Microsoft Challenge/Response	✓	N/A	N/A	✓	✓

Caracteristicile produselor	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certificări					
Cip: CC EAL6+	✓	✓	N/A	✓	✓
Certificare NIST - FIPS 140-2 L2	N/A	N/A	N/A	N/A	✓
Platformă Java: card java certificat CC EAL5+/PP	✓	✓	N/A	✓	N/A
Platformă Java + applet PKI: CC EAL5+/PP QSCD	✓	N/A	N/A	✓	N/A
eIDAS calificat atât pentru eSignature, cât și pentru eSeal	✓	N/A	N/A	✓	N/A
ANSSI francez	✓	N/A	N/A	✓	N/A
Acces fizic - configurații Mifare Classic și DesFire	N/A	N/A	✓	✓	✓
Alte caracteristici					
Politică PIN onboard	✓	N/A	N/A	✓	✓
Compatibilitate multi-PIN	✓	N/A	N/A	✓	✓
Personalizare și branding	✓	N/A	N/A	✓	✓
Sisteme de operare					
FIDO compatibil cu Windows 10 și alte sisteme de operare conforme FIDO	✓	✓	✓	✓	✓
PKI compatibil cu Windows, macOS X și Linux	✓	N/A	N/A	✓	✓

Despre managementul accesului SafeNet și soluțiile de autentificare de la Thales

Managementul accesului și soluțiile de autentificare lider în industrie de la Thales le permit întreprinderilor să gestioneze la nivel central și să securizeze accesul la aplicațiile IT, web și bazate pe cloud ale întreprinderii. Folosind SSO bazat pe politici și metode de autentificare universale, întreprinderile pot preveni în mod eficient breșele, pot migra în mod securizat în cloud și simplifica conformitatea cu reglementările.

Despre Thales

Oamenii pe care vă bazați ca să vă protejeze confidențialitatea se bazează pe Thales pentru a-și proteja datele. Când vine vorba de securitatea datelor, organizațiile se confruntă cu un număr din ce în ce mai mare de momente decisive. Indiferent dacă este momentul să vă construiți o strategie de criptare, să migrați în cloud sau să îndepliniți cerințele de conformitate, vă puteți baza pe Thales pentru a vă securiza transformarea digitală.

Tehnologie decisivă pentru momente decisive.