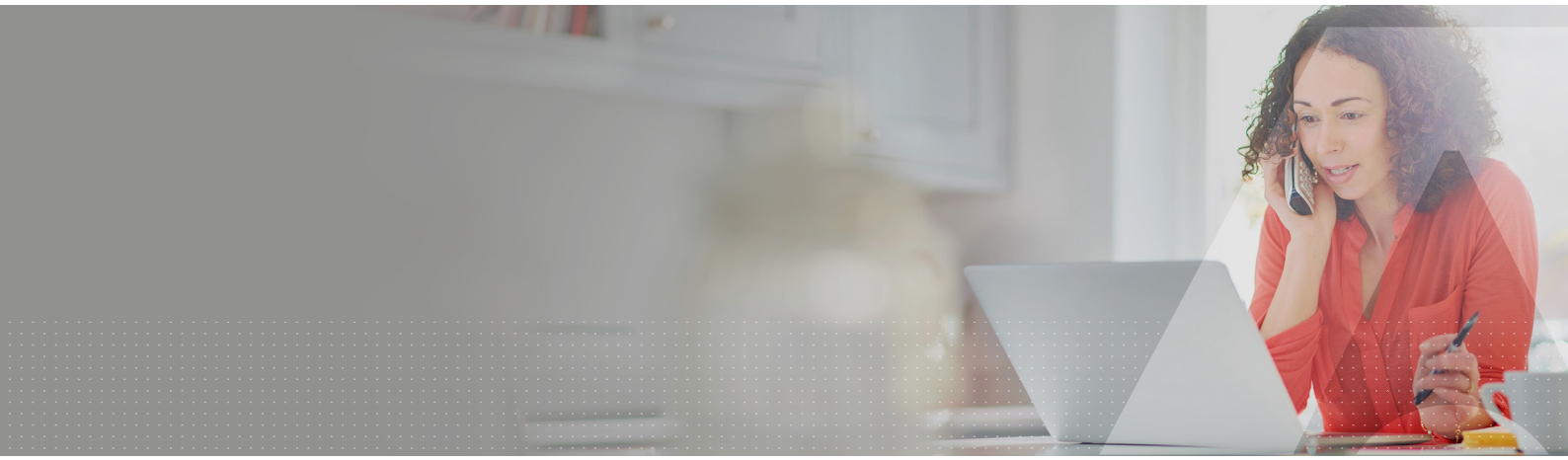
cpl.thalesgroup.com

THALES
Building a future we can all trust

SafeNet FIDO2 wachtwoordloze devices

Verlaag het risico op beveiligingsinbreuken met wachtwoordloze Multi-factor Authenticatie



Organisaties die hun digitale transformatie voortzetten, verplaatsen applicaties en gegevens naar de cloud om (1) toegankelijkheid vanaf elke locatie mogelijk te maken en (2) kosten te verlagen. Naarmate gebruikers inloggen op steeds meer cloudgebaseerde applicaties, wordt het duidelijk dat zwakke wachtwoorden de primaire oorzaak zijn van identiteitsdiefstal en beveiligingsinbreuken.

Om het risico te verlagen bij het inloggen op Windows, SaaS-applicaties voor high privilege gebruikers en voor gebruikers in het algemeen, ondersteunt Thales FIDO-wachtwoordloze authenticatie met behulp van hardware-devices met Multi-factor Authenticatie (MFA).

Door FIDO-authenticatiehardware te gebruiken in plaats van wachtwoorden, kan een moderne, compliance, wachtwoordloze MFA-ervaring worden aangeboden die bestand is tegen phishingaanvallen en accountovernames.

De Multi-factor Authenticatie-devices van Thales gebruiken moderne protocollen voor de ondersteuning van meerdere applicaties tegelijkertijd. Gebruik één sleutel die ondersteuning voor FIDO2, WebAuthn, U2F en PKI combineert om toegang te krijgen tot zowel fysieke ruimtes als IT toepassingen.

Wachtwoordloze FIDO2-authenticatie

Wachtwoordloze FIDO-authenticatie vermindert het risico op beveiligingsinbreuken door kwetsbare wachtwoorden te vervangen door FIDO-authenticatie.

FIDO-authenticatie heeft aan populariteit gewonnen als een moderne vorm van MFA vanwege de aanzienlijke voordelen. Zo wordt de inlogervaring voor gebruikers vergemakkelijkt en de inherente kwetsbaarheden van op tekst gebaseerde wachtwoorden geëlimineerd. Voordelen zijn onder meer gebruiksgemak en een hoog beveiligingsniveau.

Maakt authenticatie van meerdere gebruikers mogelijk

Thales, de wereldleider op het gebied van digitale beveiliging, ondersteunt talloze wachtwoordloze authenticatietrajecten met een krachtige reeks FIDO-devices.

FIDO met gecombineerde badge

Fysieke toegang- Voor optimaal gemak ondersteunen Thales FIDO-smartcards fysieke toegang, waardoor gebruikers met een enkele gepersonaliseerde smartcard toegang krijgen tot zowel fysieke ruimtes als IT toepassingen.

Uitbreiding van moderne authenticatie naar PKI-omgevingen - Organisaties die afhankelijk zijn van PKI-authenticatie kunnen nu een gecombineerde PKI-FIDO-smartcard gebruiken om hun cloud- en digitale transformatie te vergemakkelijken dankzij een enkel authenticatie-device voor de gebruikers ter beveiliging van de toegang tot legacy apps, netwerkdomeinen en clouddiensten.

Remote Toegang

Of men nu thuis werkt of onderweg is, gebruikers kunnen inloggen op cloudgebaseerde zakelijke applicaties vanaf meerdere devices en op meerdere locaties.

De FIDO-authenticators van Thales bieden veilige externe toegang met MFA om uw organisatie te beschermen, ongeacht het device en de locatie.

Inloggen op Windows-pc's en netwerken

De FIDO-authenticators bieden wachtwoordloze MFA, waardoor gebruikers veilig kunnen inloggen op Windows-pc's en -tablets. Met de gecombineerde FIDO PKI-kaarten kunnen we één device aanbieden om veilig in te loggen op elk besturingssysteem, met inbegrip van Windows 10, 8 en 7, Windows Server OS, macOS en Linux. Dit betekent dat organisaties de Thales FIDO-PKI-devices kunnen gebruiken voor de ondersteuning van zowel FIDO- als PKI-authenticatie en digitale handtekeningen.

Bescherm SaaS-apps

Aangezien de meeste gebruikers hun wachtwoorden opnieuw gebruiken in apps, kunt u de beveiliging drastisch verbeteren en het aantal helpdeskoproepen verminderen door gebruikers uit te rusten met FIDO-authenticators. De Thales FIDO-devices zijn volledig compatibel met Azure AD en zorgen voor veilige toegang tot Azure AD-toepassingen.

Secure Mobile Access

De Thales FIDO-devices maken moderne authenticatie op elk apparaat mogelijk door gebruikers in staat te stellen contactloos te authenticeren door middel van een eenvoudige 'tap & go' om veilige toegang te krijgen tot elke cloudbron vanaf elk mobiel apparaat.

Privileged Access Management

Privileged gebruikers met verhoogde rechten of de mogelijkheid om in te loggen op PAM-oplossingen, hebben gemakkelijke toegang tot gevoelige gegevens - hun accounts zijn het ultieme doel van kwaadwillenden.

Door privileged gebruikers multi-factor authenticatie te bieden om kwetsbare wachtwoorden te vervangen, wordt ervoor gezorgd dat alleen geautoriseerde gebruikers toegang hebben tot privileged bronnen.

IDP-compatibiliteit

SafeNet FIDO2 wachtwoordloze devices zijn compatibel met elke Identity Provider (IDP) die de FIDO2-standaard ondersteunt.

Op onze website vindt u lijst met IDP's die door ons zijn getest en gevalideerd, https://cpl.thalesgroup.com/access-management/authenticators/fido-devices

Voor alle ondernemingen, geef uw werknemers en contractanten één device voor al hun authenticatie- en toegangsbehoeften, of men nu thuis of op kantoor werkt. Geef fysieke toegang tot gebouwen en gecontroleerde gebieden en faciliteer de mobiliteit van werknemers. Overweeg uw gebruiksscenario's en kies de SafeNet FIDO-authenticators die het best aansluiten op uw behoeften.

Producteigenschappen	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Formaat	Smartcard	USB-A token	Smartcard	Smartcard	Smartcard
Contact (ISO 7816)	FIDO & PKI	n.v.t.	n.v.t.	PKI	PKI
Contactloos (ISO144443)	FIDO & PKI	n.v.t.	FIDO & Fysieke toegang	FIDO & Fysieke toegang	FIDO & Fysieke toegang
Geheugen					
Geheugenkaart	400 KB Java Flash	400 KB Java Flash	586 KB user ROM	Contactchip: 400KB Java Flash Contactloze chip: 586 KB user-ROM	Contactchip: 400KB Java Flash Contactloze chip: 586 KB user-ROM
Vrij geheugen beschikbaar voor resident-keys, certificaten, extra applets en gegevens	73 KB	90 KB	88,3 – 98,3 KB	Contact: 73 KB Contactloos: 88,3 – 98,3 KB	Contact: 73 KB Contactloos: 88,3 – 98,3 KB
Capaciteit sleutel					
FIDO resident-keys	Tot 8	Tot 8	Tot 8	Tot 8	Tot 8
PKI key-containers	20	n.v.t.	n.v.t.	20	20
Standaard ondersteund					
Java Card	3.0.4	3.0.4	n.v.t.	3.0.4	3.0.5
Wereldwijd platform 2.2.1	✔	✔	n.v.t.	✔	✔
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Basis CSP-minidriver (SafeNet minidriver)	✔	n.v.t.	n.v.t.	✔	✔
Cryptografische algoritmen (PKI)					
Hash algoritme: SHA-1, SHA-256, SHA-384, SHA-512.	✔	n.v.t.	n.v.t.	✔	✔
RSA: tot RSA 4096 bits	✔	n.v.t.	n.v.t.	✔	✔
RSA OAEP & RSA PSS	✔	n.v.t.	n.v.t.	✔	✔
P-256 bits ECDSA, ECDH. P-384 en P-521bits ECDSA, ECDH zijn beschikbaar via persoonlijke configuratie	✔	n.v.t.	n.v.t.	✔	✔
Generatie van asymmetrische sleutelparen op de kaart (RSA tot 4096 bits en elliptische krommen tot 521 bits)	✔	n.v.t.	n.v.t.	✔	✔
Symmetrisch: AES—Alleen voor beveiligde berichtenuitwisseling en 3DES voor Microsoft Challenge/ Response	✔	n.v.t.	n.v.t.	✔	✔

Producteigenschappen	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certificaties					
Chip: CC EAL6+	✔	✔	n.v.t.	✔	✔
NIST certification - FIPS 140-2 L2	n.v.t.	n.v.t.	n.v.t.	n.v.t.	✔
Java platform: CC EAL5+/ PP Java Card gecertificeerd	✔	✔	n.v.t.	✔	n.v.t.
Java platform + PKI applet: CC EAL5+/PP QSCD	✔	n.v.t.	n.v.t.	✔	n.v.t.
eIDAS gekwalificeerd voor zowel eSignature als eSeal	✔	n.v.t.	n.v.t.	✔	n.v.t.
ANSSI (Frankrijk)	✔	n.v.t.	n.v.t.	✔	n.v.t.
Fysieke toegang - Mifare Classic & DesFire-configuraties	n.v.t.	n.v.t.	✔	✔	✔
Overige kenmerken					
Onboard PIN policy	✔	n.v.t.	n.v.t.	✔	✔
Ondersteuning van meerdere pincodes	✔	n.v.t.	n.v.t.	✔	✔
Maatwerk en branding	✔	n.v.t.	n.v.t.	✔	✔
Besturingssystemen					
FIDO is compatibel met Windows 10 en andere FIDO-compatibele besturingssystemen	✔	✔	✔	✔	✔
PKI is compatibel met Windows, macOS X en Linux	✔	n.v.t.	n.v.t.	✔	✔

Over SafeNet Trusted Access, de oplossing voor toegangsbeheer en authenticatie van Thales

De toonaangevende oplossingen voor toegangsbeheer en authenticatie van Thales stellen ondernemingen in staat centraal toegang te beheren en te beveiligen tot zakelijke IT-, web- en cloudapplicaties. Door gebruik te maken van op beleid gebaseerde SSO en universele authenticatiemethoden, kunnen bedrijven inbreuken effectief voorkomen, veilig naar de cloud migreren en de naleving van regelgeving vereenvoudigen.

Over Thales

De mensen op wie u vertrouwt voor de bescherming van uw privacy, vertrouwen op Thales voor de bescherming van hun gegevens. Als het gaat om databeveiliging, krijgen organisaties te maken met steeds meer beslissende momenten. Of het nu gaat om het ontwikkelen van een encryptiestrategie, het overstappen naar de cloud of het voldoen aan nalevingsvereisten, u kunt op Thales vertrouwen voor het beveiligen van uw digitale transformatie.

Doorslaggevende technologie voor beslissende momenten.

> cpl.thalesgroup.com <

Neem contact met ons op – Ga voor alle kantoorlocaties en contactgegevens naar cpl.thalesgroup.com/contact-us