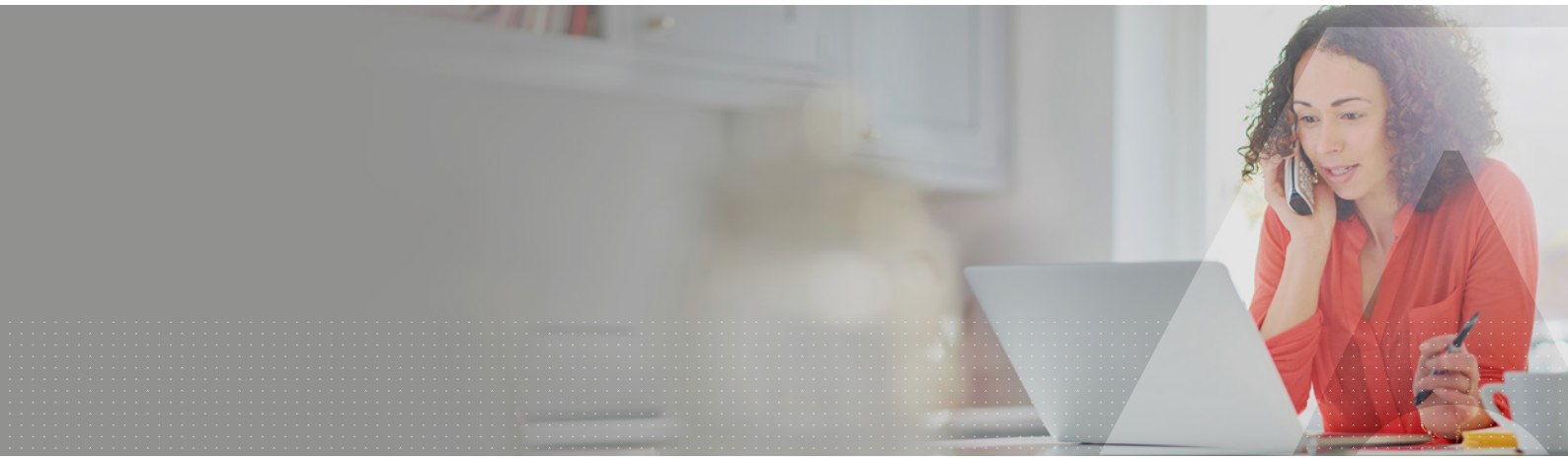
cpl.thalesgroup.com/de

THALES
Building a future we can all trust

Passwortlose SafeNet-FIDO2-Geräte

Senken Sie das Risiko von Sicherheitsverletzungen durch passwortlose Multi-Faktor-Authentifizierung



Unternehmen verlagern Anwendungen und Daten im Zuge Ihrer digitalen Transformation in die Cloud. So können sie jederzeit und von überall aus auf diese Daten und Anwendungen zugreifen und die Betriebskosten senken. Da sich Benutzer bei immer mehr unterschiedlichen Cloud-basierten Anwendungen anmelden, sind schwache Passwörter zunehmend der Hauptgrund für Identitätsdiebstahl und Sicherheitsverletzungen.

Um das Risiko für Ihre Windows-Anmeldung, SaaS-Anwendungen, privilegierten Benutzer sowie Benutzer im Allgemeinen zu senken, unterstützt Thales passwortlose Authentifizierung mithilfe von Hardwaregeräten zur Multifaktor-Authentifizierung (MFA).

Indem Sie Passwörter durch FIDO-Authentifzierungshardware ersetzen, ermöglichen Sie eine passwortlose Multifaktor-Authentifizierung, die Phishing-Angriffe und Account-Übernahmen abwehrt und Compliance gewährleistet.

Die Geräte zur Multifaktor-Authentifizierung von Thales nutzen aktuelle und zukünftige Protokolle zur gleichzeitigen Unterstützung mehrerer Anwendungen. Unterstützen Sie mit einem einzigen Schlüssel gleichzeitig FIDO2, WebAuthn, U2F und PKI und gewähren Sie so Zugang zu physischen Räumen und logischen Ressourcen.

Passwortlose FIDO2-Authentifizierung

Indem Sie anfällige Passwörter durch FIDO-Authentifizierung ersetzen, senken Sie das Risiko von Datenschutzverletzungen.

FIDO-Authentifizierung ist eine moderne Form der Multifaktor-Authentifizierung und setzt sich aufgrund ihrer erheblichen Vorteile mehr und mehr durch. Sie vereinfacht die Anmeldung für die Benutzer und beseitigt die Sicherheitslücken, die durch textbasierte Passwörter entstehen. Vorteile sind unter anderem ihre Benutzerfreundlichkeit und hohe Sicherheit.

Ermöglichen Sie mehrere Wege der Benutzerauthentifizierung

Thales, der weltweit führende Anbieter für digitale Sicherheit, unterstützt zahlreiche passwortlose Authentifizierungsmöglichkeiten mit einer Auswahl an leistungsstarken FIDO-Geräten.

FIDO mit einer einzigen Ausweiskarte

Physischer Zugang: Die individuell konfigurierbaren FIDO-Smart-Cards von Thales ermöglichen Benutzern Zugang sowohl zu physischen Räumen als aus zu logischen Ressourcen und bieten damit optimale Benutzerfreundlichkeit.

Moderne Authentifizierung auch für PKI-Umgebungen: Unternehmen, die auf PKI-Authentifizierung vertrauen, können nun eine kombinierte PKI-FIDO-Smartcard nutzen, um ihre Cloud-Einführung und digitale Transformation zu unterstützen. Damit stellen sie ihren Benutzern ein einziges Authentifizierungsgerät für sicheren Zugriff auf **ältere Anwendungen, Netzwerkdomains und Cloud-Dienste bereit.**

Fernzugriff

Unabhängig davon, ob Benutzer von Zuhause aus arbeiten oder auf Reisen sind, können sie sich von mehreren Geräten und unterschiedlichen Standorten aus in Cloud-basierte Unternehmensanwendungen einloggen.

Die FIDO-Authentifikatoren bieten sicheren Fernzugriff mittels Multifaktor-Authentifizierung und schützen Ihr Unternehmen unabhängig von Endgerät oder Standort.

Windows-PC- und Netzwerkanmeldung

FIDO-Authentifikatoren ermöglichen passwortlose Multifaktor-Authentifizierung, damit Benutzer sicher auf Windows-PCs und Tablets zugreifen können. Mit den kombinierten FIDO-PKI-Cards bieten wir ein einziges Gerät für die sichere Anmeldung bei allen Betriebssystemen einschließlich Windows 10, 8 und 7, Windows Server, macOS und Linux an. Damit können Unternehmen mit den FIDO-PKI-Geräten von Thales sowohl FIDO- und PKI-Authentifizierung als auch digitale Signaturen unterstützen.

SaaS-Apps schützen

Da Passwörter größtenteils für mehrere Apps verwendet werden, können Sie die Sicherheit dramatisch erhöhen und Anrufe beim Helpdesk vermeiden, indem Sie diese Benutzer mit FIDO-Authentifikatoren ausstatten. Die FIDO-Geräte von Thales sind vollständig mit Azure AD kompatibel und gewährleisten sicheren Zugriff auf von Azure AD verwaltete Anwendungen.

Sicherer mobiler Zugriff

Die FIDO-Geräte von Thales ermöglichen eine moderne Authentifizierung auf allen Geräten. Benutzer können sich kontaktlos durch „Tap and Go" authentifizieren und so sicher von einem beliebigen Mobilgerät aus auf alle Cloud-Ressourcen zugreifen.

Verwaltung privilegierter Benutzerzugriffe

Privilegierte Benutzer mit weitreichenden Rechten oder der Berechtigung, sich in PAM-Lösungen einzuloggen, haben freien Zugang zu sensiblen Daten. Deshalb sind ihre Accounts ein begehrtes Ziel von Angreifern.

Indem Sie dafür sorgen, dass sich privilegierte Benutzer mit Multifaktor-Authentifizierung anstatt mit für Angriffe anfälligen Passwörtern anmelden, stellen Sie sicher, dass nur berechtige Benutzer auf privilegierte Ressourcen zugreifen können.

IDP-Kompatibilität

Die passwortlosen SafeNet-FIDO2-Geräte sind mit allen Identitätsanbietern (Identity Provider, IDP) kompatibel, die den FIDO2-Standard unterstützen.

Auf unserer Website finden Sie eine Liste der IDPs, die wir getestet und gemeinsam validiert haben: https://cpl.thalesgroup.com/access-management/authenticators/fido-devices

Alle Unternehmen sollten ihren Mitarbeitern und Auftragnehmern ein einziges Geräte zur Authentifizierung und Anmeldung bereitstellen – unabhängig davon, ob diese im Homeoffice oder im Büro eingesetzt sind. Gewähren Sie physischen Zugang zu Gebäuden und kontrollierten Bereichen und fördern Sie die Mitarbeitermobilität. Betrachten Sie die konkreten Anwendungsfälle und wählen Sie den für Sie passenden SafeNet-FIDO-Authentifikator.

Produkteigenschaften	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Formfaktor	Smart Card	USB-A-Token	Smart Card	Smart Card	Smart Card
Kontakt (ISO7816)	FIDO und PKI	N/A	N/A	PKI (Public Key Infrastructure)	PKI (Public Key Infrastructure)
Kontaktlos (ISO144443)	FIDO und PKI	N/A	FIDO und physischer Zugang	FIDO und physischer Zugang	FIDO und physischer Zugang
Speicher					
Speicherchip	400 KB Java Flash	400 KB Java Flash	586 KB Benutzer-ROM	Kontaktchip: 400KB Java Flash Kontaktloser Chip: 586 KB Benutzer-ROM	Kontaktchip: 400KB Java Flash Kontaktloser Chip: 586 KB User ROM
Freier Speicherplatz für Resident Keys, Zertifikate, zusätzliche Applets und Daten	73 KB	90 KB	88,3–98,3 KB	Kontakt: 73 KB Kontaktlos: 88,3–98,3 KB	Kontakt: 73 KB Kontaktlos: 88,3–98,3 KB
Schlüsselkapazität					
FIDO Resident Keys	Bis zu 8	Bis zu 8	Bis zu 8	Bis zu 8	Bis zu 8
PKI-Schlüssel-Container	20	N/A	N/A	20	20
Unterstützte Standards					
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	✔	✔	✔	✔	✔
Base CSP Minidriver (SafeNet Minidriver)	✔	N/A	N/A	✔	✔
Kryptographische Algorithmen (PKI)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✔	N/A	N/A	✔	✔
RSA: bis zu 4096-Bit-RSA	✔	N/A	N/A	✔	✔
RSA OAEP und RSA PSS	✔	N/A	N/A	✔	✔
P-256 Bit ECDSA, ECDH. P-384 und P-521 Bit ECDSA, ECDH ist über eine benutzerdefinierte Konfiguration verfügbar	✔	N/A	N/A	✔	✔
Erstellung eine asymmetrischen Schlüsselpaares auf der Karte (RSA bis zu 4096 Bit und elliptische Kurven bis zu 521 Bit)	✔	N/A	N/A	✔	✔
Symmetrisch: AES — für sichere Nachtrichtübermittlung und 3DES nur für Challenge/Response von Microsoft	✔	N/A	N/A	✔	✔

Produkteigenschaften	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Zertifikate					
Chip: CC EAL6+	✔	✔	N/A	✔	✔
NIST-Zertifizierung: FIPS 140-2 L2	N/A	N/A	N/A	N/A	✔
Java-Plattform: CC EAL5+/ PP Java Card zertifiziert	✔	✔	N/A	✔	N/A
Java-Plattform + PKI-Applet: CC EAL5+/PP QSCD	✔	N/A	N/A	✔	N/A
eIDAS-qualifiziert für eSignature und eSeal	✔	N/A	N/A	✔	N/A
Französische ANSSI	✔	N/A	N/A	✔	N/A
Physischer Zugang: Mifare-Classic- und DesFire-Konfigurationen	N/A	N/A	✔	✔	✔
Sonstige Funktionen					
Integrierte PIN-Richtlinie	✔	N/A	N/A	✔	✔
Unterstützung von Multi-PIN	✔	N/A	N/A	✔	✔
Personalisierung und Branding	✔	N/A	N/A	✔	✔
Betriebssysteme					
FIDO wird von Windows 10 und weiteren FIDO-konformen Betriebssystemen unterstützt	✔	✔	✔	✔	✔
PKI wird von Windows, macOS X und Linux unterstützt	✔	N/A	N/A	✔	✔

Über die SafeNet-Lösungen für Zugriffsverwaltung und Authentifizierung von Thales

Mit den branchenführenden Lösungen für Zugriffsverwaltung und Authentifizierung von Thales können Unternehmen den Zugriff auf ihre IT-, Web- und Cloud-basierten Anwendungen zentral verwalten und sichern. Durch den Einsatz von richtlinienbasiertem SSO und universellen Authentifizierungsmethoden können sie effektiv Sicherheitsverletzungen verhindern, sicher in die Cloud migrieren und die Einhaltung gesetzlicher Vorschriften vereinfachen.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.

> cpl.thalesgroup.com/de <

Kontakt – Alle Bürostandorte und Kontaktinformationen finden Sie auf cpl.thalesgroup.com/contact-us