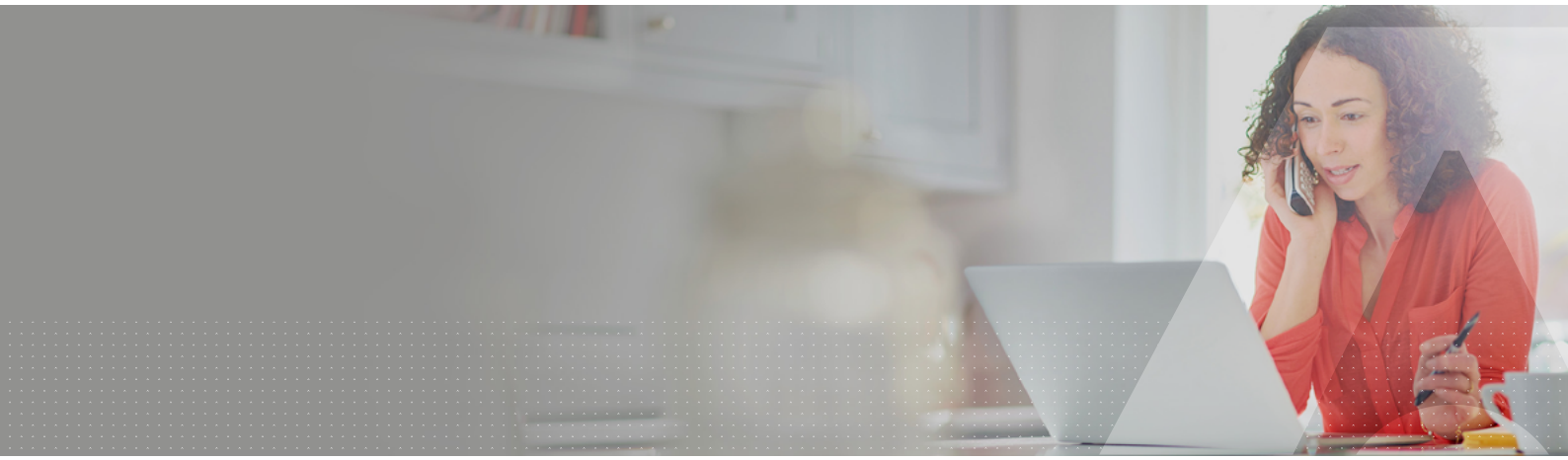
cpl.thalesgroup.com/it

THALES
Building a future we can all trust

Dispositivi senza password SafeNet FIDO2

Riduci il rischio di violazioni della sicurezza con un'autenticazione multi-fattore senza password



Le organizzazioni che espandono la propria trasformazione digitale stanno spostando applicazioni e dati nel cloud per (1) consentire gli accessi da qualsiasi luogo e (2) ridurre i costi operativi. Mentre gli utenti accedono a un numero crescente di applicazioni basate sul cloud, le password deboli si stanno rivelando essere la principale causa di furti d'identità e violazioni nella sicurezza.

Per ridurre i rischi legati agli accessi a Windows, alle applicazioni SaaS e agli utenti soprattutto se privilegiati, Thales supporta l'autenticazione FIDO senza password utilizzando dispositivi hardware di autenticazione multi-fattore (MFA).

Sostituire le password con un hardware di autenticazione FIDO introduce un'esperienza di MFA moderna, senza password, resistente agli attacchi di phishing e alle appropriazioni di account, garantendo la compliance.

I dispositivi di autenticazione multi-fattore di Thales utilizzano protocolli attuali ed emergenti per supportare svariate applicazioni allo stesso tempo. Utilizza un'unica chiave che sfrutta FIDO2, WebAuthn, U2F e PKI per accedere a spazi fisici e risorse logiche.

Autenticazione senza password FIDO2

L'autenticazione senza password FIDO riduce il rischio di violazioni nella sicurezza sostituendo password testuali vulnerabili con l'autenticazione FIDO.

L'autenticazione FIDO ha guadagnato terreno come forma moderna di MFA grazie alla sua notevole capacità di facilitare l'esperienza di accesso per gli utenti e di superare le vulnerabilità intrinseche delle password testuali. Tra i vantaggi troviamo un minore attrito per gli utenti e un livello di sicurezza più elevato.

Abilitazione di svariati processi di autenticazione

Thales, leader globale nella sicurezza digitale, supporta svariati percorsi di autenticazione senza password grazie a una solida gamma di dispositivi FIDO

FIDO con distintivo convergente

Accesso fisico: per garantire la massima comodità, le smart card FIDO di Thales supportano l'accesso fisico permettendo agli utenti di accedere sia agli spazi fisici che alle risorse logiche con un'unica smart card personalizzabile.

Estensione dell'autenticazione moderna agli ambienti PKI: le organizzazioni che si affidano all'autenticazione PKI possono ora utilizzare una smart card combinata PKI-FIDO per facilitare le iniziative di trasformazione cloud e digitale offrendo ai propri utenti un unico dispositivo di autenticazione per proteggere gli accessi ad applicazioni legacy, domini di rete e servizi sul cloud.

Accesso da remoto

Che lavorino da casa o si trovino in viaggio, gli utenti possono accedere alle applicazioni aziendali basate sul cloud da più dispositivi in sedi diverse.

Gli autenticatori FIDO di Thales forniscono un accesso sicuro da remoto con la MFA per proteggere la tua organizzazione indipendentemente dall'endpoint e dalla posizione.

Accesso a PC Windows e relative reti

Gli autenticatori FIDO forniscono una MFA senza password, consentendo agli utenti di accedere in modo sicuro a PC e tablet Windows. Grazie alle carte FIDO-PKI combinate, siamo in grado di offrire un unico dispositivo per accedere in modo sicuro a qualsiasi sistema operativo, fra cui Windows 10, 8 e 7, Windows Server, macOS e Linux. Ciò significa che le organizzazioni possono utilizzare i dispositivi FIDO-PKI di Thales per supportare le esigenze di autenticazione e firme digitali sia FIDO che PKI.

Protezione delle applicazioni SaaS

Poiché la maggior parte degli utenti riutilizza le proprie password in più applicazioni, munendo gli utenti di autenticatori FIDO, potrai migliorare drasticamente il tuo sistema di sicurezza e ridurre le chiamate al servizio di assistenza. I dispositivi FIDO di Thales sono perfettamente compatibili con Azure AD e garantiscono un accesso sicuro alle applicazioni gestite da quest'ultimo.

Protezione degli accessi da dispositivo mobile

I dispositivi FIDO di Thales consentono un'autenticazione moderna su qualsiasi dispositivo, permettendo agli utenti di autenticarsi in maniera "contactless" per ottenere un accesso sicuro a qualsiasi risorsa cloud da qualunque dispositivo mobile.

Gestione degli accessi privilegiati

Gli utenti con privilegi elevati o la possibilità di accedere a soluzioni PAM hanno accesso immediato ai dati sensibili, così che i loro account diventano l'obiettivo principale degli utenti malintenzionati.

Fornire agli utenti privilegiati un'autenticazione multi-fattore per sostituire le password vulnerabili garantisce che solo gli utenti autorizzati possano accedere a risorse privilegiate.

Compatibilità con IDP

I dispositivi senza password SafeNet FIDO2 sono compatibili con qualunque fornitore di identità (Identity Provider - IDP) che supporta lo standard FIDO2.

Per un elenco degli IDP che abbiamo testato e convalidato congiuntamente, visita il sito https://cpl.thalesgroup.com/it/access-management/authenticators/fido-devices

A prescindere dalla tipologia aziendale, puoi offrire ai tuoi dipendenti e appaltatori un dispositivo unico per ogni loro esigenza di autenticazione e accesso, sia che lavorino da casa o in ufficio. Consenti l'accesso fisico agli edifici e alle aree controllate e agevola la mobilità dei dipendenti. Considera i tuoi casi d'uso e scegli l'autenticatore SafeNet FIDO più adatto alle tue esigenze.

Caratteristiche di prodotto	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Fattore di forma	Smart card	Token USB-A	Smart card	Smart card	Smart card
Tradizionale (ISO 7816)	FIDO & PKI	N/A	N/A	PKI (infrastruttura a chiave pubblica)	PKI (infrastruttura a chiave pubblica)
Contactless (ISO144443)	FIDO & PKI	N/A	FIDO & accesso fisico	FIDO & accesso fisico	FIDO & accesso fisico
Memoria					
Chip di memoria	Java Flash 400 KB	Java Flash 400 KB	ROM dell'utente 586 KB	Chip tradizionale: Java Flash 400 KB Chip contactless: ROM utente 586 KB	Chip tradizionale: Java Flash 400 KB Chip contactless: ROM utente 586 KB
Memoria libera disponibile per chiavi residenti, certificati, applet e dati aggiuntivi	73 KB	90 KB	88,3 – 98,3 KB	Tradizionale: 73 KB Contactless: 88,3 – 98,3KB	Tradizionale: 73 KB Contactless: 88,3 – 98,3KB
Capacità della chiave					
Chiave residente FIDO	Fino a 8	Fino a 8	Fino a 8	Fino a 8	Fino a 8
Container di chiavi PKI	20	N/A	N/A	20	20
Standard supportati					
Carta Java	3.0.4	3.0.4	N/A	3.0.4	3.0.5
Piattaforma globale 2.2.1	✔	✔	N/A	✔	✔
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Minidriver base CSP (minidriver SafeNet)	✔	N/A	N/A	✔	✔
Algoritmi di crittografia (PKI)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✔	N/A	N/A	✔	✔
RSA (fino a 4096 bit)	✔	N/A	N/A	✔	✔
RSA OAEP & RSA PSS	✔	N/A	N/A	✔	✔
P-256 bit ECDSA, ECDH. P-384 & P-521bit ECDSA, ECDH disponibili con configurazione personalizzata	✔	N/A	N/A	✔	✔
Generazione di coppie di chiavi asimmetriche su carta (RSA fino a 4096 bit & curve ellittiche fino a 521 bit)	✔	N/A	N/A	✔	✔
Simmetrica: AES per messaggi sicuri e 3DES esclusivamente per Microsoft Challenge/Response	✔	N/A	N/A	✔	✔

Caratteristiche di prodotto	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certificati					
Chip: CC EAL6+	✔	✔	N/A	✔	✔
Certificazione NIST - FIPS 140-2 L2	N/A	N/A	N/A	N/A	✔
Piattaforma Java: certificato CC EAL5+ / PP	✔	✔	N/A	✔	N/A
Piattaforma Java + applet PKI: CC EAL5+/PP QSCD	✔	N/A	N/A	✔	N/A
Conformità a eIDAS per firme e sigilli elettronici	✔	N/A	N/A	✔	N/A
ANSSI francese	✔	N/A	N/A	✔	N/A
Accesso fisico: configurazioni MIFARE classic e DESFire	N/A	N/A	✔	✔	✔
Altre funzionalità					
Integrazione PIN	✔	N/A	N/A	✔	✔
Assistenza multi-PIN	✔	N/A	N/A	✔	✔
Personalizzazione e branding	✔	N/A	N/A	✔	✔
Sistemi operativi					
Supporta FIDO in Windows 10 e altri sistemi operativi conformi a FIDO	✔	✔	✔	✔	✔
PKI supportata in Windows, macOS X e Linux	✔	N/A	N/A	✔	✔

Scopri di più sulle soluzioni per la gestione degli accessi e l'autenticazione SafeNet di Thales

Thales offre soluzioni leader nel settore per la gestione degli accessi e l'autenticazione per permettere alle aziende di gestire e proteggere in maniera centralizzata l'accesso alle applicazioni aziendali di tipo IT, web e basate sul cloud. Utilizzando SSO basate su criteri e metodi di autenticazione universali, le aziende possono efficacemente prevenire violazioni, migrare nel cloud in sicurezza e semplificare gli obblighi di compliance.

Informazioni su Thales

Le persone a cui ti affidi per tutelare la tua privacy si affidano a Thales per proteggere i propri dati. Le organizzazioni si ritrovano ad affrontare sempre più spesso momenti decisivi in materia di sicurezza dei dati. Qualunque sia l'obiettivo del momento, dal creare una strategia di crittografia al passare al cloud o garantire il rispetto degli obblighi di compliance, puoi contare su Thales per proteggere la tua trasformazione digitale.

Tecnologia decisiva per momenti decisivi.

> cpl.thalesgroup.com/it <

Contattaci – per tutti i recapiti e per conoscere l'ubicazione dei nostri uffici, visita cpl.thalesgroup.com/contact-us