cpl.thalesgroup.com

THALES
Building a future we can all trust

Autentificarea FIDO

Manual

Cuprins

Parolele nu sunt viabile

Profesioniștii din domeniul securității IT din toată lumea sunt de acord că parolele sunt învechite și că ar trebui considerate ca fiind niște relicve ale trecutului. Costurile de întreținere a parolelor depășesc beneficiile. Parolele devin din ce în ce mai previzibile și îi lasă pe utilizatori vulnerabili în fața furtului și compromiterii parolelor. Chiar și cele mai puternice parole pot fi supuse phishingului. Motivele pentru eliminarea mecanismelor de autentificare bazate pe parole sunt covârșitoare.

Pentru departamentele IT ale companiilor, susținerea și întreținerea parolelor reprezintă o povară care crește costurile biroului de asistență, creează complexitate și conduce la experiențe neplăcute ale utilizatorilor în legătură cu cerințele de resetare a parolelor. Mai presus de toate, parolele nu mai sunt adecvate pentru a oferi protecție împotriva amenințărilor de securitate cibernetică actuale și nu corespund nevoilor corporative de securitate a informațiilor.

Rapoartele privind brețele de date indică faptul că infractorii cibernetici profită de parolele nesecurizate pentru a lansa atacuri împotriva organizațiilor. Parolele compromise, furate sau slabe sunt un vector cheie pentru atacurile reușite de divulgare a datelor cu caracter personal, de preluare a site-urilor web și conturilor legitime ale utilizatorilor. Astfel de atacuri pot avea consecințe grave pentru companii și indivizi deopotrivă.

61%

din brețele de date implică acreditări. Utilizarea incorectă a privilegiilor reprezintă principalul tip de utilizare incorectă în brețele de date.

Utilizarea incorectă a privilegiilor reprezintă principalul tip de utilizare incorectă în brețele de date. Acreditările reprezintă principalul tip de date compromise în brețele de date.

39%

din organizații s-au confruntat cu o creștere a atacurilor de tip „credential stuffing” (testarea unui număr mare de acreditări compromise) și a altor atacuri asupra parolelor

Organizațiile trebuie să depășească momentul simplei utilizări a parolelor pentru autentificarea utilizatorilor și protejarea datelor.

Ce este FIDO2?

Deși în prezent există numeroase soluții pentru implementarea autentificării fără parole, Fast Identity Online (FIDO2) promite să ofere un mecanism de autentificare cu adevărat simplu și securizat.

Standardul FIDO2 are rolul de a soluționa scenarii cu mai mulți utilizatori pentru simboluri criptografice multifactor, fără parole. Un autentificator FIDO2, cunoscut, de asemenea, sub denumirea de cheie de securitate FIDO, încorporează una sau mai multe chei private, fiecare dedicată unui singur cont online. Protocoalele solicită un „gest al utilizatorului" — un cod PIN, o metodă biometrică sau un simbol de autentificare — înainte de a putea fi folosită cheia privată pentru a semna un răspuns la o provocare de autentificare.

Cheile de securitate FIDO2 pot înlocui integral acreditările slabe pe bază de parole statice cu acreditări puternice hardware sau software pe bază de chei publice/private.

Avantajele FIDO2

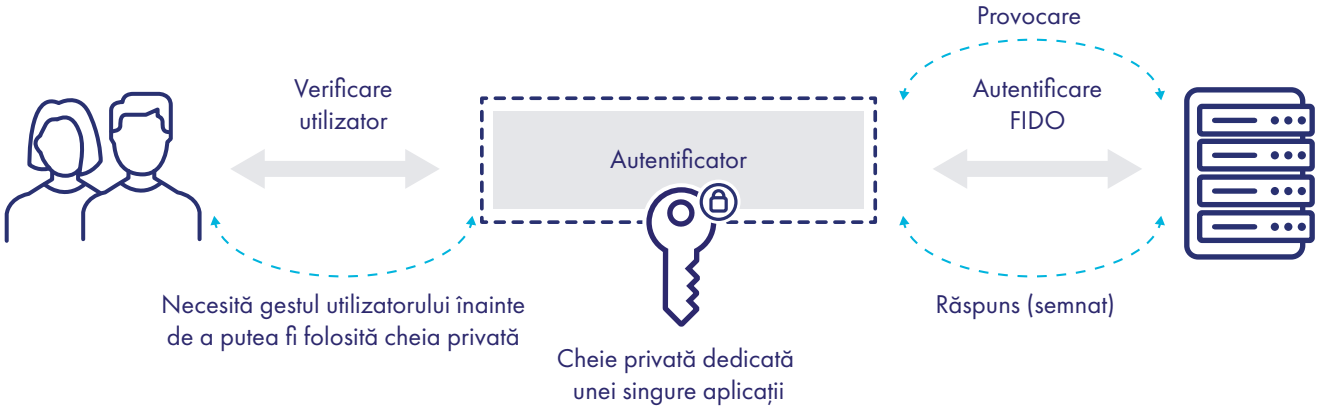
Securitatea: Acreditări unice de autentificare pe fiecare site web, care nu sunt niciodată stocate pe un server, ceea ce elimină riscurile de phishing, toate formele de furt al parolelor și atacurile prin repetare.

Experiența utilizatorului: Utilizatorii se autentifică cu metode încorporate simple pe dispozitivele lor sau folosind chei de securitate FIDO2 ușor de utilizat.

Confidențialitate: Chei unice pentru fiecare site internet, care nu pot fi folosite pentru a urmări utilizatorii pe alte site-uri. Atunci când sunt utilizate, datele biometrice nu părăsesc niciodată dispozitivul utilizatorului.

Scalabilitate: Activarea FIDO2 printr-o simplă apelare JavaScript API care este acceptată pe toate browserele și platformele de top.

Cum lucrează FIDO?



FIDO2 și conformitatea cu reglementările

Companiile sunt reglementate de o rețea tot mai complexă de reguli, jurisdicții și standarde care impun cerințe de securitate și confidențialitate. Un numitor comun al tuturor reglementărilor îl constituie nevoia de autentificare puternică.

Conformitatea cu GDPR și CCPA

Potrivit ambelor reglementări, subiecții datelor, cetățeni ai UE și Statului California, au drepturi de acces, corectare, ștergere și portabilitate privind datele lor cu caracter personal. O componentă cheie pentru furnizarea în mod securizat a acestor capacități este asigurarea autenticității și validității identității indivizilor care exercită aceste drepturi privind datele.

Standardul FIDO2 și dispozitivele compatibile respectă protecția datelor cu caracter personal și permit o autentificare simplificată, dar, totuși, eficientă. FIDO2 se bazează pe criptografia cheilor publice, iar cheile sunt generate și stocate local pe dispozitivul de autentificare, fără secrete partajate pe server. Răspunsul de autentificare este criptat, oferind protecție împotriva phishingului și atacurilor de interpunere, în timp ce datele biometrice sunt stocate și prelucrate doar pe dispozitivul utilizatorului.

Conformitatea cu PSD2

Directiva Uniunii Europene privind serviciile de plată (PSD2) are rolul de a crea o piață europeană integrată a plăților, care să facă plățile mai sigure și mai securizate, pentru a-i proteja pe consumatori. Una dintre cerințele cheie ale directivei PSD2 este nevoia de autentificare puternică a clienților (SCA) folosind factori multipli de autentificare, unde „breșa la nivelul unuia dintre elemente nu compromite fiabilitatea celorlalte elemente."

Băncile și furnizorii de servicii de plată pot profita de dispozitivele acreditate FIDO2 pentru a respecta cerințele de conformitate ale Autorității Bancare Europene. Utilizarea criptografiei asimetrice contribuie la combaterea tuturor atacurilor cunoscute care vizează acreditările „partajate", cum ar fi parolele. Datele biometrice și cheile de securitate utilizate sunt o dovadă a factorilor de autentificare de tipul „ce ești" și „ce ai", fiind mult mai comode pentru utilizatori.

Respectarea cerințelor specificate de Ordinul executiv al S.U.A. privind securitatea cibernetică

Secțiunea 3.d a Ordinului executiv solicită implementarea autentificării multifactor. Dispozitivele FIDO Thales și alte opțiuni de autentificare oferă cea mai vastă gamă de soluții de autentificare și factori de formă, permițând agențiilor federale și statale să respecte cerințele esențiale de autentificare și zero trust specificate în Ordinul executiv al S.U.A.

Considerente practice

Trebuie să înlocuim metodele de autentificare existente?

Pentru a gestiona numărul din ce în ce mai mare al îngrijorărilor privind securitatea accesului, multe organizații au investit în scheme de autentificare puternică, inclusiv autentificare pe bază de PKI și hardware sau soluții mobile OTP. Nu este practic pentru ele din punct de vedere al costului sau operațional să dezinstaleze și să înlocuiască aceste soluții, mai ales dacă acestea vin în întâmpinarea nevoilor companiei.

Organizațiile trebuie să evalueze toate soluțiile de autentificare disponibile pentru a afla care soluție satisface diversele cazuri de utilizare.

	Dispozitive FIDO2	Hardware OTP	Aplicație OTP Push/OTP Mobile	Cartele inteligente X.509	SMS
Conectare în rețea	Ridicat	Mediu	Mediu	Ridicat	Scăzut
Acces cloud/VPN	Ridicat	Ridicat	Ridicat	Scăzut	Scăzut
Acces privilegiat	Ridicat	Ridicat	Ridicat	Ridicat	Scăzut

Soluțiile, inclusiv cele oferite de Thales, acceptă o gamă variată de metode, tehnologii și factori de formă de autentificare. Aceste soluții le permit organizațiilor să securizeze adoptarea cloud și să concilieze accesul securizat în medii hibride printr-o ofertă integrată de autentificare și management al accesului, facilitând inițiativele lor de transformare cloud și digitală prin faptul că le oferă propriilor utilizatori un singur dispozitiv de autentificare pentru securizarea accesului la aplicațiile vechi, domeniile de rețele și serviciile cloud.

Combinarea autentificării PKI cu autentificarea FIDO2

Multe organizații au investit în infrastructura cu chei publice (PKI) pentru a gestiona autentificarea pe bază de certificate. Impusă de numeroase reglementări privind securitatea și confidențialitatea și de standarde care necesită un nivel înalt de garanție și o autentificare puternică, PKI este utilizată în general de industrii și organizații, inclusiv bănci, spitale, furnizori de energie și alții, pentru a securiza accesul la date și aplicații.

Din cauza complexității gestionării certificatelor digitale și infrastructurii PKI, companiile sunt adesea forțate să facă compromisuri între funcționalitatea și securitatea afacerii, ceea ce poate crea breșe grave și le poate expune la atacuri cibernetice.

Organizațiile care au investit în PKI pentru autentificarea și accesul securizat la aplicațiile tradiționale nu trebuie să își dezinstaleze sau înlocuiască mediul de autentificare existent. Dimpotrivă, ele pot suplimenta PKI cu FIDO2, pot porni de la infrastructura lor existentă și își pot extinde amprenta de securitate existentă la metode de autentificare moderne pentru a proteja accesul la aplicații bazate pe cloud.

Avantaje

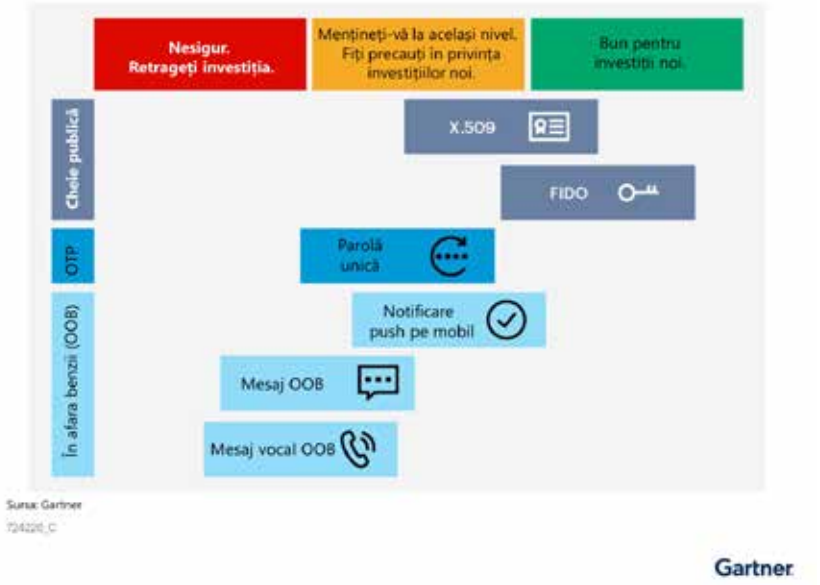
- Autentificare unificată și soluție de securizare a accesului atât pentru aplicațiile vechi, cât și pentru cele moderne, precum și pentru datele bazate pe cloud.
- Integrare mai rapidă în aplicații pentru autentificare puternică, bazată pe criptografia cheilor publice ale protocolului FIDO2.
- Costuri mai mici pentru companii, deoarece pot porni de la infrastructura lor de autentificare existentă și își pot extinde mecanismele de autentificare.
- Conformitatea cu legislațiile privind confidențialitatea pentru toate cazurile de utilizare, pentru a asigura faptul că informațiile private și sensibile sunt protejate și preveni orice fel de expunere neautorizată a acestor date.
- Complexitate redusă pentru utilizatorii finali, dezvoltatori și administratori.

Investirea în soluții care sunt pregătite pentru viitor

Gartner® anticipează că până în 2025, mai mult de 25% din tranzacțiile MFA care folosesc un simbol se vor baza pe protocoale de autentificare FIDO, în creștere de la mai puțin de 5% în prezent. În plus, Gartner le recomandă liderilor din domeniul securității și al managementului riscurilor să evalueze cu atenție ce opțiuni se potrivesc cel mai bine cu nevoile lor tactice și strategice și:

- Să optimizeze valoarea investițiilor prin alegerea unor metode care pot oferi o autentificare a utilizatorilor consecventă, adecvată, rezonabilă și eficientă.
- Să se asigure că metodele de autentificare (cu sau fără simboluri) respectă aceste criterii prin evaluarea nivelului de încredere, a costului total al deținerii, a experienței utilizatorilor (UX) și a altor nevoi și constrângeri în diferite cazuri de utilizare.
- Să reducă vulnerabilitățile potențiale în implementările vechi, retrăgându-și investiția în moduri OOB vechi, dovedite ca fiind slabe, cum ar fi SMS și să migreze la metode mai eficiente.
- Să planifice îmbunătățirea consecvenței în multiple cazuri de utilizare, pregătindu-se pentru investiții strategice în FIDO2, căutând oportunități tactice de investiții în viitorul apropiat.

Valoarea strategică a diferitelor tipuri de simboluri de autentificare



Sursa: Gartner, Innovation Insight for Many Flavors of Authentication Token, Ant Allan, David Mahdi, Tricia Phillips, mai 2021. GARTNER este o marcă comercială înregistrată și o marcă de servicii deținută de Gartner, Inc. și/sau afiliații săi în S.U.A. și la nivel internațional, fiind utilizată în această publicație pe bază de permisiune. Toate drepturile rezervate.

Avantajul FIDO Thales

Gama completă de dispozitive FIDO

Există mulți furnizori care oferă diverse simboluri de autentificare. Cu toate acestea, numai Thales oferă o gamă completă de dispozitive FIDO pentru a gestiona toate cazurile posibile de utilizare pentru autentificare. În mod specific, dispozitivele SafeNet FIDO Thales includ:

- Cartele inteligente PKI-FIDO pentru a gestiona atât cazurile de utilizare PKI, cât și FIDO
- Cartele inteligente FIDO cu compatibilitate NFC, care acceptă autentificarea FIDO prin intermediul dispozitivelor mobile
- Cartele inteligente FIDO cu acces logic combinat, care permit cazuri de utilizare combinate pe bază de ecuson – acces logic
- Dispozitive USB FIDO cu detectarea prezenței, ce permit accesul securizat de la distanță la serviciile cloud

Integrarea completă cu Azure AD

Toate dispozitivele FIDO Thales sunt complet compatibile și integrate cu serviciile gestionate Azure AD. Dispozitivele SafeNet FIDO le oferă utilizatorilor o experiență de conectare unitară și fără parole, de pe toate dispozitivele. Organizațiile care utilizează dispozitivele FIDO2 Thales pot gestiona cazuri de utilizare noi, menținând, în același timp, echilibrul optim între securitate și comoditate cu autentificarea fără parole.

Pentru informații suplimentare și pentru a afla ce recomandă Gartner, citiți raportul „Innovation Insight for Many Flavors of Authentication".

THALES

Building a future we can all trust

Contactați-ne

Pentru toate locațiile birourilor și informațiile de contact, vizitați cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <