

**VARNOSTNI KLJUČ YUBICO YUBIKEY
FIDO2 U2F, USB-A, NFC, ČRN****43,99€****SKU:** FIDO2-U2F-BLK**Kategorije:** [Računalniški deli](#), [USB oprema](#)**OPIS IZDELKA****ZDRUŽLJIVOST**

Yubico Security Key deluje z napravami, ki jih poganjajo operacijski sistemi Windows, macOS, ChromeOS in Linux. Podpira vse popularne spletne brskalnike, na stotine različnih storitev in izbrane upravitelje gesel. Priključi se lahko na USB-A 1.0, 2.0 ali 3.0 vhod, za uporabo z

VZDRŽLJIVOST

Security Key je odporen na vodo in prah po standardu IP68. Zunanost ključka je izdelana iz plastike ojačane s steklenimi vlakni, katera je bolj odporna na zvijanje, lomljenje in udarce. Za svojo uporabo ne potrebuje baterij ter nima gibljivih delov.

MOČNA AVTENTIKACIJA

Ključek omogoča enostaven vpis v aplikacije in lahko nadomesti uporabo gesel. Prav tako pa se ga lahko uporabi za izboljšanje varnosti z uporabo za dvo- ali več-faktorsko avtentikacijo. Podpira FIDO2/Webauthn in FIDO



mobilnimi napravami pa lahko uporabite NFC, ki je podprt na sodobnih Android in iOS napravah. ali v ZDA po najvišjih varnostnih standardih.

Osrednje lastnosti

- Močna prvo- ali več-faktorska strojna avtentikacija - lahko nadomesti gesla
- Enostavna avtentikacija z dotikom gumba na ključku ali približanjem NFC napravi
- Ne potrebuje nobene dodatne programske opreme ali gonilnikov
- Deluje na Windows, macOS, ChromeOS in Linux operacijskih sistemih ter večjih brskalnikih s FIDO2 ali U2F podporo
- Ne vsebuje baterij ali premikajočih delov
- Nizka teža s 3 grami ter visoka odpornost proti obrabi, vodi in udarcem

Več o FIDO U2F standardu

FIDO Universal 2nd Factor je uveljavljen odprt avtentikacijski standard s privzeto podporo na različnih platformah in v brskalnikih. YubiKey FIDO2 U2F podpira neomejeno število internetnih storitev, pri čemer do ponudnikov storitev ne pošilja nobenih informacij o uporabnikih ali šifrirnih ključev.

Več o FIDO2 standardu

FIDO2 je odprt avtentikacijski standard, ki sestoji iz W3C Web Authentication (WebAuthn API) in Client to Authentication protokola (CTAP). Slednji je aplikacijski protokol, ki se uporablja za komunikacijo



med odjemalcem (brskalnik) ali platforme (operacijski sistem) ter zunanjim avtentikaterjem (varnostni ključ Yubico).

FIDO 2 nudi enako raven zaščite kot FIDO U2F, saj je prav tako zasnovan na šifriranju z javnim ključem. Poleg tega, da se pri avtentikaciji obnaša kot drugi faktor, pa lahko tudi popolnoma nadomesti gesla (prvi faktor) z močnimi strojno generiranimi ključi. Teh ključev pa ni mogoče ponovno uporabiti ali deliti med storitvami, zato ne morejo biti tarča phishinga, "Man in the middle" napadov ali vdorov v strežnike.

Yubico je glavni sodelujoči pri CTAP protokolu, patent pa je v lasti FIDO Alliance.

Tehnične podrobnosti

- Varnostne funkcije: WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F)
- Deluje z: Google računi, Microsoft računi, Salesforce.com, Keeper, 1Password, Bitwarden Premium, Dropbox, Facebook, Twitter, AWS Identity and Access Management (IAM), Duo Security, Forgerock, Idaptive, Microsoft Azure AD, Okta, OneLogin, Ping Identity, iCloud,...
- Certifikati: FIDO Universal 2nd Factor (U2F), FIDO2, IP68, FIDO L2
- Komunikacija: USB-A in NFC
- Metode šifriranja: ECC p256