Alternativa geslom – FIDO2 in Passkey

Marko Hölbl, Marko Kompara

Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko,
Maribor, Slovenija
marko.holbl@um.si, marko.kompara@um.si

Gesla, ki so najpogostejši način overjanje uporabnikov na spletu, imajo številne pomanjkljivosti in jih zato pogosto označujemo kot Ahilova peta varnosti. Zato se venomer pojavljajo težnje k odpravi gesel in eden izmed pomembnih korakov v to smer je overjanje brez gesel (ang. passwordless authentication) s pomočjo tehnologije Passkey, ki je nastala pod okriljem zavezništva FIDO in poveznim standardom FIDO2. Passkey ponuja izpopolnjen in na uporabnika osredotočen pristop k overjanju brez gesel. V bistvu gre za kriptografski par ključev, varno shranjen na uporabnikovi napravi, z možnostjo uporabe na več napravah in operacijskih sistemih ter shranjevanjem v varnih elementih naprav (kot so TPM ali varne enklave). S tem je postopek overjanje poenostavljen, tako da uporabnikom omogoča overjanje s preprostim biometričnim skeniranjem ali overjanje na podlagi naprave, s čimer odpravi potrebo po pomnjenju in upravljanju gesel. Tako Passkey predstavlja naslednji korak v razvoju informacijske varnosti, saj zagotavlja zanesljiv okvir, ki odpravlja pomanjkljivosti tradicionalnih metod overjanja, hkrati pa je usklajen z varnostnimi in uporabnostnimi cilji sodobnih digitalnih komunikacij. V okviru prispevka se bomo osredotočili na predstavitev pojmov, povezanih z overjanjem brez gesel, standardom FIDO2 ter s poudarkom na delovanju tehnologije Passkey. Prav tako bodo predstavljene prednosti in varnostne funkcionalnosti omenjene tehnologije.

Ključne besede:
Overjanje
Gesla
FIDO 2
Passkey
WebAuthn

Univerzitetna založba Univerze v Mariboru
ISBN 978-961-286-894-9
DOI https://doi.org/10.18690/um.feri.4.2024.16

1 Uvod

Gesla so najpogostejši način overjanje uporabnikov na spletu. Vendar imajo več pomanjkljivosti. Na vprašanje o geslih veliko ljudi odgovori, da si jih je težko zapomniti, da jih je lahko pozabiti, da pogosto povzročajo težave ter so zato označena kot Ahilova peta varnosti. Uporabniki namreč pogosto ponovno uporabijo ista gesla za več računov ali pa izberejo šibka gesla, ki jih napadalci lahko uganejo. Poleg tega lahko overjanje z uporabniškim imenom in geslom zahteva dodatne korake, kot je dvofaktorsko overjanje (ang. Two-Factor Authenticartion – 2FA), s čimer se poveča varnost, vendar je postopek prijave za uporabnika tudi bolj zapleten [1].

Leta 2022 je bilo 90 % spletišč tarča napadov z zvabljanjem (ang. phishing), vsako drugo geslo pa je bilo ponovno uporabljeno za dostop do različnih spletnih računov, kot navaja zavezništvo FIDO (ang. FIDO - Fast IDentity Online Alliance) [2]. Povprečen uporabnik ima več kot 100 računov, ki zahtevajo gesla, večina pa za prijavo v večino storitev uporablja isto geslo (ali nekaj gesel). S slabimi navadami glede izbire in/ali uporabe gesel ogrožamo svoje osebne podatke. Uporabniki pogosto na tak način ogrožajo svojo varnost zavoljo prikladnosti oz. enostavnejše uporabe. Vsak četrti Američan uporablja običajna gesla, kot so Abc123, Password1111 in P@ssw0rd. Dve tretini jih priznava, da uporabljajo isto šibko geslo na več spletnih mestih, zaradi česar so vsi ti računi ranljivi [3]. Da bi zmanjšali tveganja in preprečili krajo podatkov, je priporočljivo, da se izogibamo ponovni uporabi poverilnic, izberemo močna gesla in jih takoj spremenimo, če je v storitvi, v kateri smo registrirani, zaznamo uhajanje podatkov.

Gesla so simptom večje težave - naše zgodnje neuspešno prepoznavanje in preverjanje identitete uporabnikov na internetu od samega začetka. Mnogi menijo, da so poverilnice, ki temeljijo na znanju (npr. gesla, kode PIN), eden od prvih grehov interneta [4]. Od takrat poskušamo krpati luknje, gesla pa so bila preprosto najmanj slaba možnost, ki nam je omogočala zavarovati po en račun naenkrat. Alternativne možnosti - strojni žetoni, telefonsko overjanje, biometrija - niso delovale, kot bi morale ali pa niso bile ekonomsko upravičene. Že omenjeno dvofaktorsko overjanje je trenutno uveljavljena metoda za povečanje varnosti.

Zaradi teh varnostnih izzivov, s katerimi se soočajo posamezniki in podjetja, se je pojavil nov standard, ki obljublja hitrost, preprostost in zanesljivost.

Za reševanje teh vprašanj je bilo ustanovljeno zavezništvo FIDO, ki je pripravilo standarda FIDO UAF in U2F ter kasneje FIDO2 [5]. Del standarda FIDO2 je tudi standard WebAuthn, ki je nastal v sodelovanju z W3C [6], [7]. FIDO so prvotno ustanovili Google, Apple in Microsoft in je namenjen zamenjavi gesel s preprostejšim, uporabniku prijaznim varnostnim sistemom, odpornim proti napadu z zvabljanjem. Z overjanjem FIDO se uporabniki prijavijo s poverilnicami, ki so odporne proti napadom z zvabljanjem in se imenujejo ključi. Ti se lahko povežejo s platformo ali varnostnim ključem in omogočajo, da se prijave samo z geslom nadomestijo z varnimi in hitrimi izkušnjami prijave na spletnih mestih in v aplikacijah. Tako omenjeni standardi in specifikacije vzpostavljajo univerzalno metodo za overjanje uporabnikov brez gesel z uporabo kriptografije javnih ključev [8]. Poverilnice, ustvarjene s to metodo, omogočajo uporabnikom, da se overjajo izključno z uporabo svoje naprave in funkcij, kot je biometrija. Tako si ni treba zapomniti več zapletenih gesel ali opraviti dodatnega koraka za potrditev identitete z dvo ali večfaktorskim overjanjem.

Passkey je tip digitalne poverilnice, ki se uporablja za overjanje, ne da bi bilo treba uporabljati običajna gesla in je trenutno najbolj razširjena in dodelana izvedba standarda FIDO2. Uporablja par kriptografskih ključev, ki so edinstveni za vsako spletno storitev. Uporabnikov varnostni ključ (skladen s standardom FIDO2), mobilni telefon ali namizni/prenosni računalnik z ustreznimi komponentami (npr. Windows Hello) je uporabnikov ključ Passkey in ju lahko uporabljam za overjanje in prijavo.

2 Overjanje brez gesel

Metoda, ki jo običajno uporabljamo za overjanje na spletnih mestih in v mobilnih aplikacijah, se je sčasoma razvila in vključuje izboljšane mehanizme zaščite. Običajno je postopek takšen, da račun ustvarimo, tako da navedemo uporabniško ime, običajno e-poštni naslov, in geslo, ki mora izpolnjevati različna merila (prisotnost velikih črk, številk, posebnih znakov itd.). Ko se želimo prijaviti, vnesemo te identifikacijske podatke. Programska koda v ozadju te podatke potrdi, in če so pravilni, zagotovi na primer žeton za dostop, ki bo nato omogočil dostop do zaščitene vsebine. Ta mehanizem se pogosto uporablja za overjanje na digitalnih platformah. Pogosto se omenjeno metodo, zaradi povečane varnosti, dopolni z dvofaktorskim overjanje, na primer s pomočjo enkratnih gesel, poslanih preko sporočil SMS, ali generiranih z namenskimi (mobilnimi) aplikacijami, kot je Google Authenticator [9].

Upravljanje identifikacijskih podatkov (ustvarjanje, spreminjanje, brisanje računov itd.) se v osnovi izvaja na strani strežnika. Vendar ima ta pristop svoje izzive. Uporabniki na primer pogosto ponovno uporabljajo ista gesla na več spletnih mestih, zato da si jih lažje zapomnijo. Ta navada skupaj z napadi, ki vodijo v krajo podatkov, identitete ali vdore, predstavlja resno varnostno tveganje. Druga dobro znana grožnja je napad z zvabljanjem, pri katerem goljufi podvajajo videz legitimnega spletnega mesta, da bi uporabnika zavedali in goljufivo zbrali njegove podatke. Tradicionalna gesla so torej občutljiva na krajo, kar vključuje tudi napade z beleženjem tipkanja (ang. keylogging attack), opazovanjem (ang. shoulder surfing) ipd. Ukradena gesla je mogoče ponovno uporabiti kasneje in na drugih napravah.

Ob upoštevanju teh dejstev je jasno, da tradicionalna kombinacija uporabniškega imena in gesla ne zadostuje več za zagotavljanje varnega overjanja.

2.1. Načini overjanja brez gesel

Leta 2013 je bilo ustanovljeno zavezništvo Fast IDentity Online Alliance (FIDO), ki združuje tehnološka podjetja, vladne agencije, ponudnike storitev (ang. relaying party), finančne institucije in druge deležnike [10]. Glavni cilj tega zavezništva je razviti standarde za overjanje z namenom zmanjšati uporabo gesel in hkrati izboljšali standarde za overjanje na spletu.

Prva izmed standardov sta bila FIDO UAF in FIDO U2. To je mogoče doseči z zagotavljanjem, da zasebni ključi in biometrični podatki, kjer je to primerno, vedno ostanejo na uporabnikovi napravi. Tako je mogoče overjanje opraviti z metodami, kot sta biometrija ali vnos enkratne kode PIN, ne da bi si bilo treba zapomniti zapleteno geslo. FIDO podpirajo tudi glavni brskalniki in operacijski sistemi. Kasneje je bil predstavljen standard FIDO2, ki je naslednik FIDO UAF, in FIDO U2F ter je odprti standard overjanja brez gesel. FIDO2 omogoča preprostejše in močnejše overjanje z uporabo kriptografije javnega ključa. Standard FIDO2 sestavljajo specifikacija W3C za spletno overjanje, API WebAuthn in protokol CTAP2.

FIDO2 definira overjanje z uporabo javnih in zasebnih ključev, pri čemer je zasebni ključ, shranjen na uporabnikovi napravi, javni ključ pa na strežnikih ponudnika storitve. Za overjanje na spletu se uporablja lokalno overjanje (npr. biometrija na telefonu). Tako se uporabniki prijavijo s prepoznavo obraza, prstnega odtisa (torej biometrično) ali z vnosom kode PIN v lokalno napravo za spletno registracijo in overjanje. To odklene zasebni ključ, shranjen na napravi, ki se zatem uporabi za overjanje pri ponudniku storitve.

Najbolj pomembni standarde, razviti pod okriljem zavezništva FIDO so:

FIDO UAF (ang. Universal Authentication Framework):

- Predstavljen leta 2014
- Omogoča overjanje brez gesel z uporabo lokalnih metod biometričnega preverjanja (kot sta prepoznavanje prstnih odtisov ali obraza) neposredno na napravi, ne da bi se biometrični podatki prenašali po omrežju.
- Uporablja se predvsem za mobilne naprave, kjer so na voljo biometrični senzorji.

FIDO U2F (ang. Universal Second Factor)

- Predstavljen leta 2014
- Zagotavlja mehanizem dvofaktorsko overjanje, ki dopolnjuje tradicionalne sisteme, ki temeljijo na geslih. Predvideva uporabo fizičnih varnostnih ključev (USB, NFC) kot drugi faktor, pri čemer mora uporabnik za overjanje izvesti aktivnost (npr. fizično vstaviti ključev v napravo).
- Namenjen izboljšanju varnosti spletnih aplikacij z dodajanjem standardiziranega drugega faktorja pri overjanju.

FIDO2 (ang. Fast IDentity Online 2):

- Predstavljen leta 2018.
- Namenjen overjanju brez gesel in dvofaktorskemu overjanju, s poudarkom na skalabilnosti in spletni združljivosti.
- Sestavljen iz:
  - **WebAuthn (ang. Web Authentication) -** API za spletno overjanje. Omogoča spletnim aplikacijam, da overjanje uporabljajo poverilnice z javnim ključem.
  - **CTAP2 (ang. Client to Authenticator Protocol)** - omogoča komunikacijo med odjemalskimi napravami (kot so pametni telefoni ali računalniki) in zunanjimi overitelji (kot so varnostni ključi).
- Zagotavlja enoten pristop k overjanju brez gesel in večfaktorsko overjanje na različnih napravah in platformah.

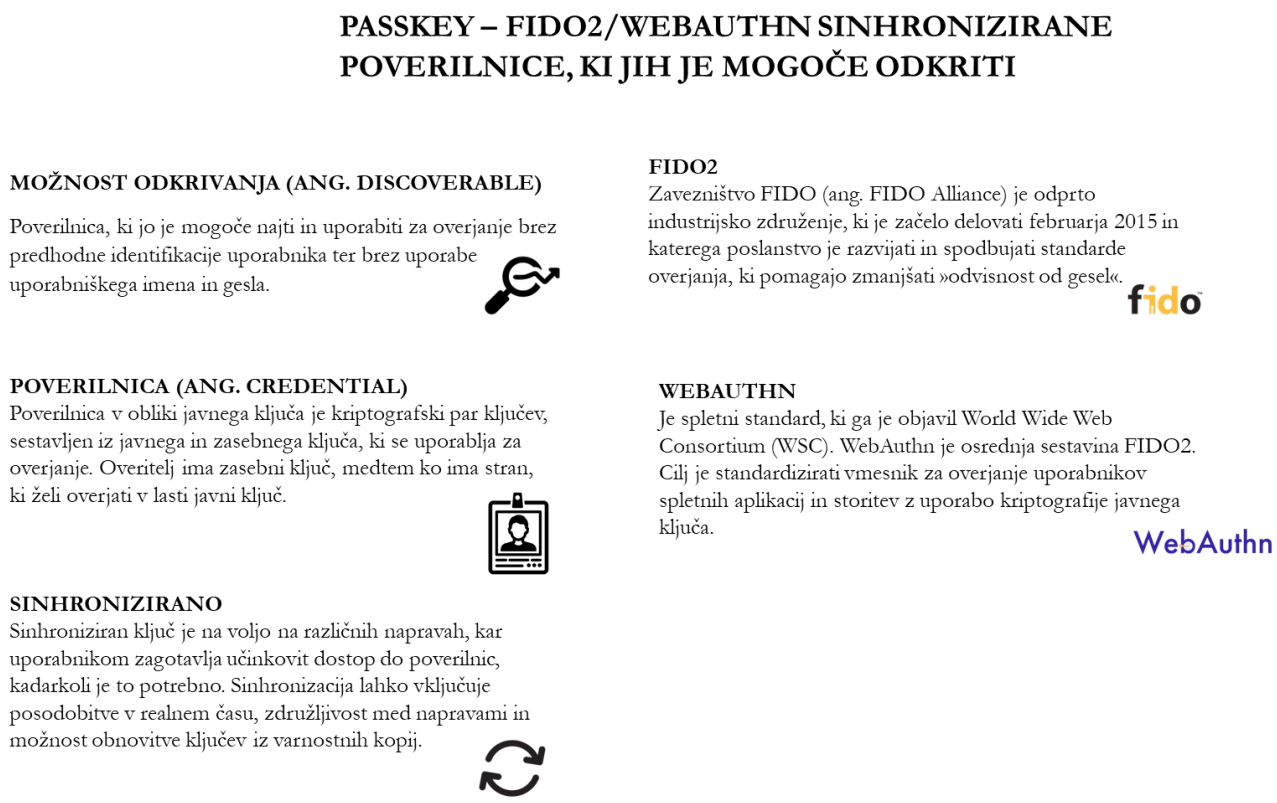
FIDO2 podpira večina platform, kot so Windows 10 in 11, Android, iOS ter brskalniki, kot so Google Chrome, Mozilla Firefox, Microsoft Edge in Apple Safari. Primeri notranjih FIDO overiteljev vključujejo Touch ID, Face ID, čitalniki prstnih odtisov ali Windows Hello. Prav tako standard podpira t.i. zunanje overitelje, kot so precej poznani Yubico ključki. Več informacij je na voljo na [11].

2.2. Najbolj znano utelešenje standarda FIDO2 - Passkey

Passkeys je najbolj znana in razširjena realizacija standarda FIDO2 s poudarkom na dobri uporabniški izkušnji. Uporabnikom omogočajo, da se overijo na različnih napravah in na različnih platformah. Zasnovan je za uporabo na več napravah in operacijskih sistemih ter se pogosto povezuje s storitvami v oblaku za sinhronizacijo vseh uporabnikovih naprav.

Passkey temelji na načelih preprostosti, učinkovitosti in varnosti:

- **Preprostost** - takojšnja vzpostavitev računa. Maprava je odgovorna za ustvarjanje poverilnic in ni potrebe po pomnjenju - overitvene kode, povezane z zasebnimi ključi, so shranjene samo v napravah določenega uporabnika. Pristopne ključe je mogoče deliti med različnimi napravami. Lahko se uporablja sinhronizacijo – npr. z oblakom. Naprave tako delujejo kot upravitelji gesel in za vas hranijo vse informacije.
- **Učinkovitost** - gesla se ustvarijo hitro in jih je mogoče sinhronizirati med različnimi napravami.
- **Varnost -** po svoji naravi so uporabljeni ključi robustni in edinstveni, kar odpravlja tveganja, povezana s ponovno uporabo gesla. Strežniki imajo dostop samo do javnih ključev. Za dostop do zasebnega ključa je potrebna biometrično overjanje. Če pride do ogrožanja podatkov na enem spletnem mestu, to ne vpliva na druga spletna mesta ali storitve, saj je vsak ključ gesla drugačen.



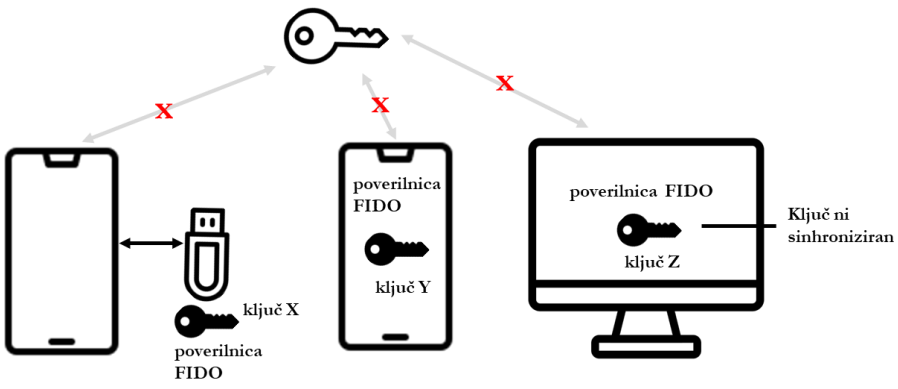
Slika 1: Pregledna infografika tehnologije Passkey.

3 Podobnosti o tehnologiji Passkey

Passkey je izraz, ki se uporablja za opis poverilnic, ki jih je možno odkrivati (ang. discoverable credentials) in so skladne s standardom FIDO2 ter uporabljajo kriptografijo javnega ključa. Uporablja se lahko za overjanje uporabnika pri ponudniku storitve brez potrebe po uporabniškem imenu in geslu. Zasebni ključ in ID poverilnice sta shranjena v overitelju, medtem ko sta javni ključ in ID poverilnice shranjena pri ponudniku storitev.

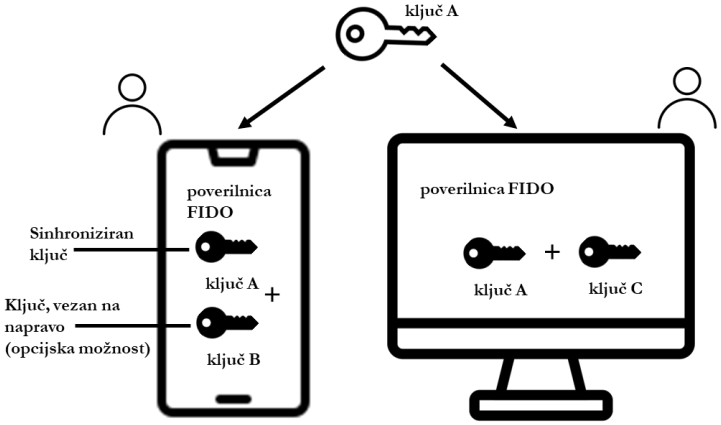
Passkey je naslednji korak v razvoju digitalnega overjanja, ki temelji na standardih zavezništva FIDO. Za razliko od gesel si uporabnikom ni treba zapomniti zapletenih nizov znakov, s čimer se izniči tveganje za napade z zvabljanjem in tako poveča raven varnosti. Obstajata dve vrsti ključev, ki ustrezata različnim potrebam in scenarijem uporabnikov.

– **Passkey za eno napravo (ang. Single-Device Passkeys)**
  Ključ je vezan na eno overitveno napravo in ne more zapustiti naprave.



Slika 2: Passkey za eno napravo. [6]

- **Passkey za več naprav (ang. Multi-Device Passkeys)**
  Ključ je mogoče sinhronizirati med različnimi uporabniškimi napravami.



Slika 3: Passkey za več naprav. [6]

Vodilni ponudniki tehnologije so naredili korak naprej pri vključevanju funkcionalnosti Passkey ključev v svoje ekosisteme. Kot primer navedimo mobilne platforme Android in iOS. Za tiste v ekosistemu Apple se ključi brez težav sinhronizirajo med napravami, povezanimi z istim AppleID-jem, in iCloud Keychain [12]. Na operacijskem sistemu Android se ključi Passkey sinhronizirajo preko računov Google, kar poenostavi dostop v različnih napravah [13]. V primerih, ko sinhronizacija v oblaku ni izvedljiva, je mogoče, da uporabniki na eni napravi ustvarijo kodo QR, in jo optično preberejo z drugo napravo, v kateri so shranjeni ključi, ter tako olajšajo prijavo v aplikacijo.

Ko je ustvarjen nov par javnih/zasebnih ključev in povezan z uporabnikom, se lahko uporabnik overi s podpisom izziva, ki ga pošlje ponudnik storitve (strežnik). Pri tem uporabi zasebni ključ, shranjen v t.i. overitelju. Za izvedbo te operacije je potrebna identifikacija uporabnika, npr. z biometričnimi podatki ali kodo PIN naprave. Z vidika uporabnika to pomeni, da lahko priročno dostopa do storitve z uporabo biometrične prepoznave ali kode PIN pametnega telefona, ne da bi si moral zapomniti več gesel (ali se zanašati na upravitelja gesel).

Poleg tega lahko uporabnik po registraciji gesla za storitev (npr. na pametnem telefonu) do nje dostopa z različnimi odjemalci na isti napravi (splet, mobilna aplikacija) ali celo na drugi napravi (drug pametni telefon, prenosni računalnik itd.).

Ena od glavnih prednosti sinhroniziranih ključev je možnost souporabe med različnimi uporabnikovimi napravami. To uporabnikom omogoča, da obnovijo svoje ključe iz varnostne kopije ali uporabijo isti ključ za overjanje na več platformah. Ta uporabniku prijazna funkcija ublaži težave, ki se lahko pojavijo pri uporabi overitvenega sredstva, vezanega na napravo. V tem primeru sinhronizacija ali varnostno kopiranje nista mogoča, saj poverilnic ni mogoče prenesti iz naprave. To lahko povzroči težave uporabniku, če fizično napravo izgubi ali zamenja.

Čeprav je ta funkcija privlačna z vidika uporabnosti in uporabniške izkušnje, je treba opozoriti, da v primerjavi z overiteljem, vezanim na napravo, nekoliko zmanjša varnost overjanja. Ključ, vezan na napravo, ne omogoča izvoza ustvarjenega ključa na zunaj naprave, kar preprečuje možnost kraje in onemogoča izkoriščanje ranljivosti, povezanih z uporabo oblaka.

Potrebno je omeniti, da specifikacija WebAuthn ne zagotavlja protokola za varnostno kopiranje zasebnih ključev poverilnic ali njihovo izmenjavo med overitelji. Zato je odgovornost za izvajanje politik varnostnega kopiranja prepuščena ponudnikom storitve (kot sta Apple ali Google v primeru ključev, ustvarjenih na mobilnih napravah). Ti ponudniki se bodo morali sami odločiti, kako bodo izvajali politike varnostnega kopiranja, kar bo na koncu

vplivalo na raven varnosti ključa, saj je ta neposredno odvisna od ravni varnosti postopka obnovitve računa, ki se uporablja za varnostno kopiranje ključev. Vendar je ta kompromis potreben, da lahko uporabniki obnovijo svoje registrirane ključe iz varnostne kopije.

3.1. Delovanje

Na tem mestu bomo obravnavali podrobnosti delovanje tehnologije Passkey. Glavni subjekti, ki so vključeni v ta tok, so:

- **uporabnik**, ki želi dostopati do storitve,
- **odjemalec**, spletno mesto ali mobilna aplikacija, ki uporabniku omogoča dostop do storitve, ki jo zagotavlja ponudnik storitve,
- **overitelj,** naprava, ki ustvarja in potrjuje kriptografske ključe, povezane z uporabnikovim ključem, ter tako zagotavlja celovitost postopka overjanja in
- **ponudnik storitve,** ki potrdi pristnost identitete uporabnika na podlagi ključa in tako odloči o dostopu do zahtevane storitve.

Ti subjekti medsebojno sodelujejo, da bi uporabniku omogočili registracijo novega ključa. Uporabnik lahko nato ta ključ uporablja za identifikacijo in dostop do ponujenih storitev v vseh nadaljnjih interakcijah.

Postopek registracije

Prva aktivnost, ki jo opravi uporabnik, je registracija v storitev z ustvarjanjem novega ključa. Možna sta dva primera:

1. Uporabnik je že registriran v storitev z uporabniškim imenom, geslom in prijavo 2FA ter želi dodati overjanje s Passkeyem. Po prijavi s klasičnim načinom bo imel možnost, da doda poverilnico tipa Passkey (ang. Passkey credential).
2. Storitev uporabnikom omogoča, da se registrirajo in povežejo novo poverilnico tipa Passkey. V tem primeru bosta ustvarjanje novega uporabnika in Passkeya potekala hkrati.

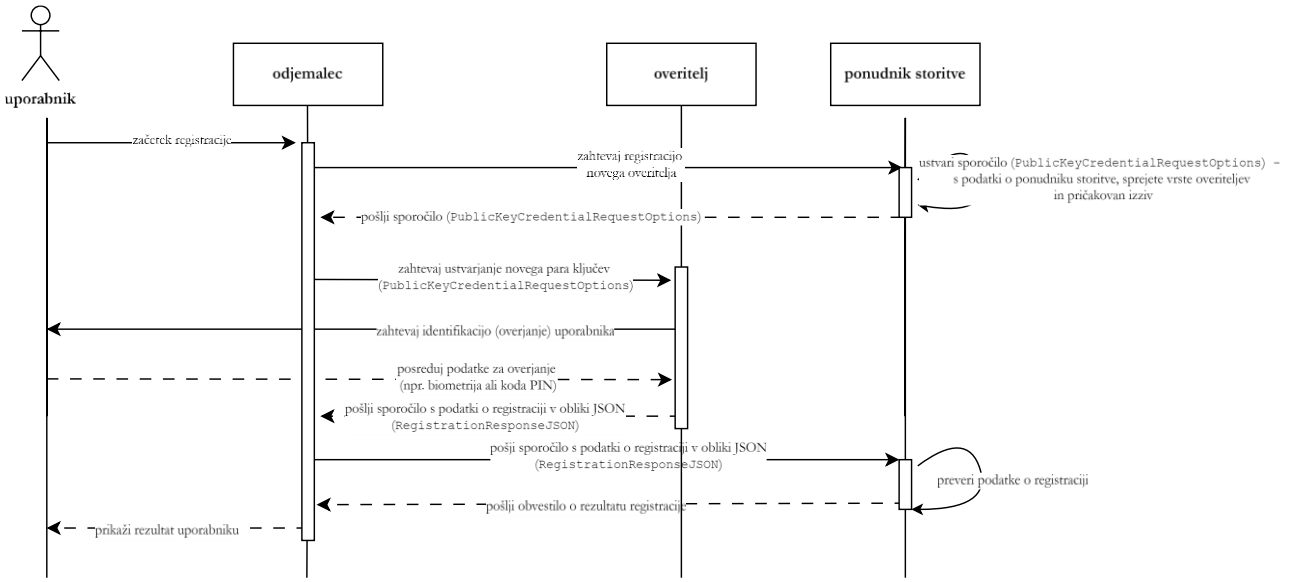
Čeprav se lahko zaledna logika pri obravnavi teh dveh scenarijev nekoliko spremeni, postopek registracije v obeh primerih ostane dosleden. Ta postopek poveže geslo s storitvijo in omogoči nadaljnji dostop.
Koraki, vključeni v postopek, so naslednji

- Uporabnik se namerava registrirati v storitev z uporabo odjemalca, bodisi mobilne aplikacije bodisi spletnega mesta.
- Odjemalec začne postopek registracije in od uporabnika zahteva, da registrira novega overitelja.
- Ponudnik storitve se odzove s sporočilom v obliki JSON (`PublicKeyCredentialRequestOptions`), ki vključuje izziv in dodatne metapodatke, kot so podatki o ponudniku storitve in sprejete vrste overiteljev. Poleg tega ponudnik storitve shrani izziv za to sejo registracije, saj ga bo treba preveriti ob prejemu odgovora.
- Odjemalec s tem odgovorom od overitelja zahteva, da ustvari nov par ključev, ki se bo uporabil za overjanje uporabnika pri ponudniku storitve.
- Overitelj (ki je lahko zunanja naprava ali naprava, na kateri se izvaja odjemalec) preveri sporočilo od strežnika in zahteva identifikacijo uporabnika (z biometričnimi podatki ali kodo PIN naprave).
  - Če je vse v redu, overitelj ustvari nov par zasebnega in javnega ključa ter odjemalcu vrne sporočilo v obliki JSON (`RegistrationResponseJSON`), ki vsebuje novo ustvarjeni javni ključ, informacije o potrditvi in druge pomembne podrobnosti. Opozoriti je treba, da zasebni ključ ostane v overitelju,

v primeru pametnih telefonov pa je shranjen v ločeni strojni komponenti (npr. v Secure Enaclave napravo na iPhoneih).

- Odjemalec potrditev pošlje ponudniku storitve, da potrdi novo registracijo.
- Ponudnik storitve preveri prejeto sporočilo in overi potrditev ter zagotovi, da registracija uporabnika izpolnjuje določena merila (npr. pravilen odgovor na izziv, ustrezna oblika potrditve).
- Po preverjanju sporočila o registraciji ponudnik storitve obvesti uporabnika o rezultatu. Če je uspešen, shrani ustrezne podatke o registrirani poverilnici, ki se bodo uporabljali za prihodnja overjanja.

Celoten postopek je tudi prikazan na Sliki 4.



Slika 4: Postopek registracije. [2]

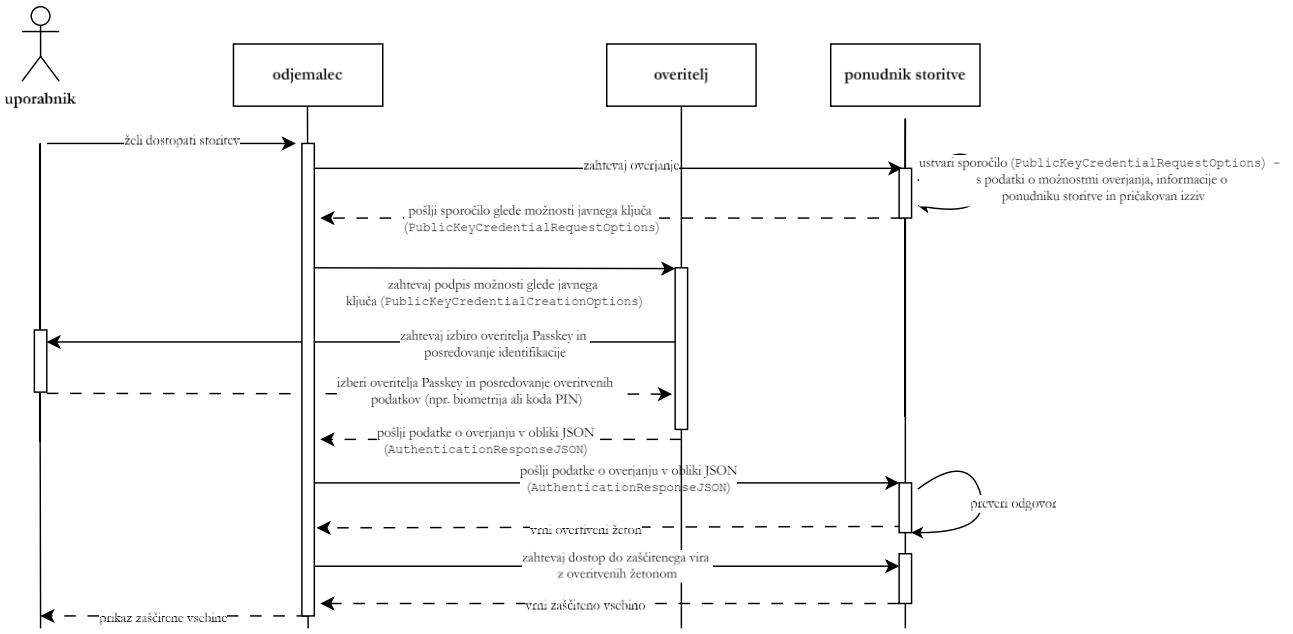
Postopek overjanja

Po uspešni registraciji lahko uporabnik uporabi Passkey za overjanje pri ponudniku storitve in dostop do zaščitenega vira. Oglejmo si postopek:

- Uporabnik želi dostopati do storitve prek mobilne aplikacije ali spletnega mesta in se mora overiti.
- Odjemalec sproži postopek overjanja tako, da od ponudnika storitve zahteva overjanje.
- Ponudnik storitve pošlje sporočilo v obliki JSON (`PublicKeyCredentialRequestOptions`), z možnostmi overjanja, ki vključujejo izziv in informacije o ponudniku storitve. Poleg tega shrani izziv za to sejo overjanja, saj ga bo treba preveriti ob prejemu odgovora.
- Odjemalec pošlje to sporočilo overitelju in zahteva, da ga podpiše z enim od ključev, povezanih z uporabnikom.
- Če ima overitelj več ključev, povezanih z uporabnikom, je ta pozvan, naj izbere ključ, da nadaljuje postopek overjanja. Ko ga izbere, se uporabnika pozove, naj zagotovi overjanje z biometričnimi podatki ali kodo PIN naprave, da se izziv podpiše z zasebnim ključem, shranjenim v overitelju.
- Če se postopek uspešno izvede, overitelj odjemalcu vrne sporočilo v obliki JSON (`AuthenticationResponseJSON`), ki vsebuje podpisan izziv, podatke o overitelju in druge ustrezne podatke odjemalca.
- Odjemalec pošlje ta odziv za overjanje ponudniku storitve.
- Ponudnik storitve najprej preveri, ali je uporabljeni overitelj registriran. Nato overi odgovor in pravilnost odgovora na izziv.

- Po uspešnem preverjanju ponudnik storitve uporabniku odobri dostop in mu omogoči uporabo storitve, pri čemer mu vrne, na primer overitveni žeton, ki se lahko uporabi za naslednje zahteve.
- Uporabnik je overjen in lahko uporablja mobilno aplikacijo ali spletno mesto.

Celoten postopek je tudi prikazan na Sliki 5.



Slika 5: Postopek overjanja. [2]

Celoten postopek je tudi prikazan na Sliki 5.

4 Zaključek

Passkey je obetavna rešitev za overjanje brez gesel. Uporabnikom ponuja standarden, priročen in varen način dostopa do storitve, ne da bi si morali zapomniti ali vnesti geslo. Od leta 2016, ko je bil objavljen prvi osnutek specifikacije FIDO (UAF in U2F), pa vse do danes, smo priča razcvetu uporabe in Passkeya bi lahko potencialno revolucionarno spremenili overjanje uporabnikov.

Vendar pa tehnologija Passkey ni brez izzivov. Čeprav se zdi zamisel o prihodnosti brez gesel privlačna, pomeni veliko spremembo, na katero se bodo uporabniki morali prilagoditi. Mnogi med njimi se morda ne zavedajo te možnosti ali njenega delovanja, zato bo morda potrebno nekaj časa in truda, da jih prepričamo, da preidejo iz overjanja z gesli. Poleg tega trenutno ni interoperabilnosti med ključi, ustvarjenimi na različnih platformah, in do zdaj ni možnosti prenosa ključa, ustvarjenega v telefonu iPhone, in sinhroniziranega prek storitve iCloud, v napravo z operacijskim sistemom Android in obratno. Vendar se tudi na tem področju obeta rešitev. Ponudniki t.i. upravljavcev gesel (ang. Password managers) že uvajajo možnost uporabe omenjenih orodij za upravljanje s ključi Passkey [14]. Tako je trenutno prihodnosti precej obetavna.

Literatura

[1] D. Coffin, "Two-factor authentication," in *Expert Oracle and Java Security: Programming Secure Oracle Database Applications with Java*, Springer, 2011, pp. 177–208.

[2] "Passkeys (Passkey Authentication)." Accessed: Jul. 30, 2024. [Online]. Available: https://fidoalliance.org/passkeys/

[3] Harris Poll, "The United States of P@ssw0rd$."

[4] Matt Kapko, "Security has an underlying defect: passwords and authentication." Accessed: Jul. 31, 2024. [Online]. Available: https://www.cybersecuritydive.com/news/security-defect-passwords-authentication/693471/

[5] "FIDO2 - FIDO Alliance." Accessed: Jul. 30, 2024. [Online]. Available: https://fidoalliance.org/fido2/

[6] P. Heim and F. Alliance, "Everybody Is Invited: How FIDO Addresses a Full Range of Use Cases," 2022.

[7] N. Frymann, D. Gardham, F. Kiefer, E. Lundberg, M. Manulis, and D. Nilsson, "Asynchronous remote key generation: An analysis of yubico's proposal for W3C webauthn," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 939–954.

[8] M. E. Hellman, "An overview of public key cryptography," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 42–49, 2002.

[9] A. Nash, H. Studiawan, G. Grispos, and K.-K. R. Choo, "Security Analysis of Google Authenticator, Microsoft Authenticator, and Authy," in *International Conference on Digital Forensics and Cyber Crime*, Springer, 2023, pp. 197–206.

[10] "FIDO Alliance Member Companies & Organizations." Accessed: Jul. 31, 2024. [Online]. Available: https://fidoalliance.org/members/

[11] G. Eleftherios, "FIDO2 Overview, Use Cases, and Security Considerations," Athens University of Economics and Business, 2023.

[12] "Passkeys Overview - Apple Developer." Accessed: Jul. 30, 2024. [Online]. Available: https://developer.apple.com/passkeys/

[13] "Passwordless login with passkeys | Authentication | Google for Developers." Accessed: Jul. 30, 2024. [Online]. Available: https://developers.google.com/identity/passkeys

[14] Inga Valiaugaitė, "Best Passkey Password Manager in 2024." Accessed: Aug. 01, 2024. [Online]. Available: https://cybernews.com/best-password-managers/passkey-password-managers/