Mobilna aplikacija
Rekono OnePass

Verzija 2.0.0

Uporabniški priročnik

Rekono d.o.o.

December 2020

Kazalo

Opis aplikacije

Aplikacija Rekono OnePass omogoča lažji in hitrejši dostop do računa Rekono, njegovo uporabo, upravljanje ter dostop do ostalih storitev Rekono.

Aplikacija je razvita v skladu z najnovejšimi razvojnimi standardi, torej vključuje in uporablja vse funkcionalnosti in senzorje, ki jih ponujajo naprave (biometrično avtentikacijo, skeniranje kode QR z uporabo fotoaparata naprave, potisna obvestila in druge varnostne mehanizme).

Omogoča večji nadzor nad uporabniškim računom Rekono ter izboljšan in hitrejši mehanizem dvofaktorske avtentikacije. Z implementacijo potisnih obvestil se lahko s klikom na gumb hitreje prijavite v svoje račune Rekono s pomočjo svojih naprav, kar pomeni hitrejši, če ne celo najhitrejši mehanizem dvofaktorske avtentikacije, ki je dodobra zavarovan s pomočjo kode PIN ali biometrične avtentikacije naprave uporabnika, če jo ta podpira.

Aplikacija Rekono OnePass ima preprost in uporabniku prijazen vmesnik, ki nudi dober pregled nad podatki o računu, geslih OTP in nastavitvah aplikacije, ki jih lahko uporabnik poljubno prilagodi svojim željam in potrebam.

Enkratna gesla so sedaj precej bolje vidna na glavnem zaslonu aplikacije, ko se prijavite v svoj račun Rekono. Privzeto se enkratno geslo Rekono samodejno vpiše, ko se uporabnik prijavi v aplikacijo in registrira napravo, tako da ga ni mogoče izbrisati. Izbriše se šele takrat, ko se uporabnik odjavi, saj takrat izginejo vsi podatki o aplikaciji (nastavitve, enkratna gesla, prilagoditve …).

Enkratno geslo lahko dodate ročno ali pa samodejno, tako da preberete kodo QR z aplikacijo za branje kod na svojem telefonu. To omogoča enostavnejše in hitrejše dodajanje enkratnih gesel v aplikacijo Rekono OnePass. Ročno dodajanje enkratnih gesel je še vedno podprto, ko mora uporabnik dodati OTP skrivnost in ime, s katerim bo enkratno geslo prikazano na glavnem zaslonu.

Aplikacija omogoča prilagoditve nastavitev, tem, jezikov in varnostnih nastavitev glede na želje, potrebe in preference uporabnikov.

Navodila za namestitev

Platforma Android

Predpogoj: S svojim računom Gmail morate biti prijavljeni v trgovino Google Play Store.

Če imate napravo z operacijskim sistemom Android, prenesete aplikacijo Rekono OnePass, tako da vpišete “Rekono OnePass” v trgovini Google Play Store, in si naložite aplikacijo v svojo napravo.

Do aplikacije lahko dostopate tudi s pomočjo brskalnika na svojem računalniku, tako da kliknete povezavo: **https://play.google.com/store/apps/details?id=si.rekono.onepass.v2**

Platforma iOS

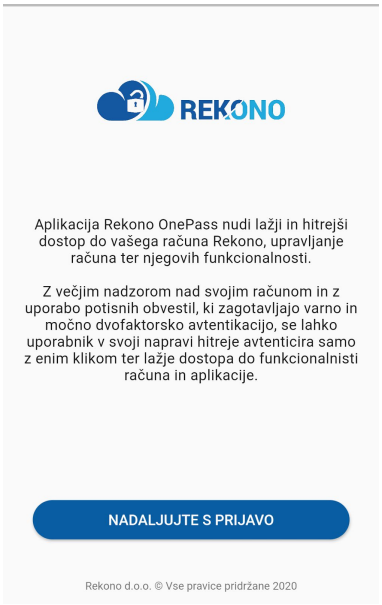
Če imate napravo z operacijskim sistemom Apple iOS, prenesete aplikacijo Rekono OnePass, tako da vpišete ‘’Rekono OnePass’’ v trgovini Apple App Store, in si naložite aplikacijo v svojo napravo.

Do aplikacije lahko dostopate tudi s pomočjo brskalnika na svojem računalniku, tako da kliknete povezavo:
https://apps.apple.com/us/app/rekono-onepass/id1502085202

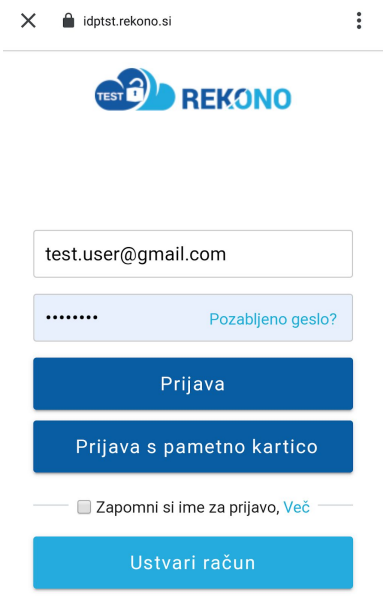
Prva uporaba in registracija

Sledi navodilo za prvo namestitev aplikacije Rekono OnePass na mobilni napravi ter navodilo za registriranje naprave v račun Rekono.

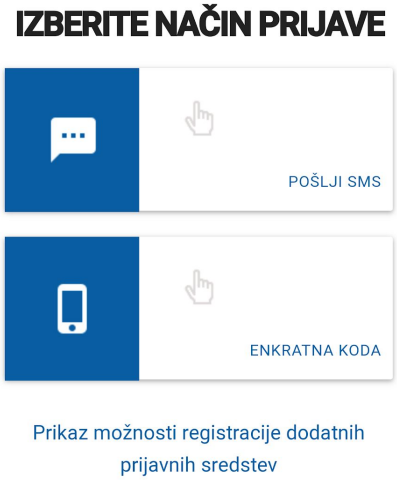
1. Zaženite aplikacijo (potrebna je aktivna internetna povezava). Prikaže se spodnji zaslon.



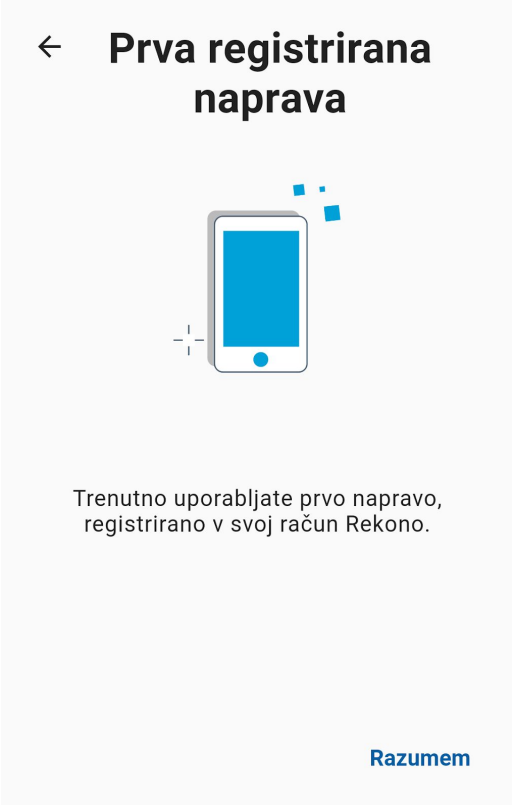
2. Kliknite gumb za nadaljevanje prijave v svoj račun Rekono, ter vpišite svoje prijavne podatke.



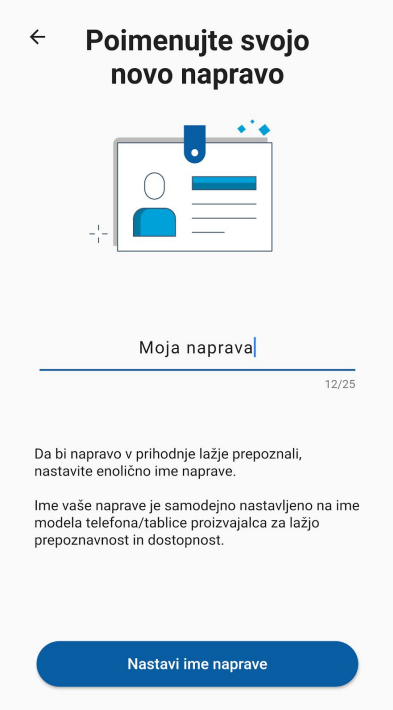
3. Po vpisu prijavnih podatkov izberite metodo dvofaktorske avtentikacije in nadaljujte avtentikacijo.



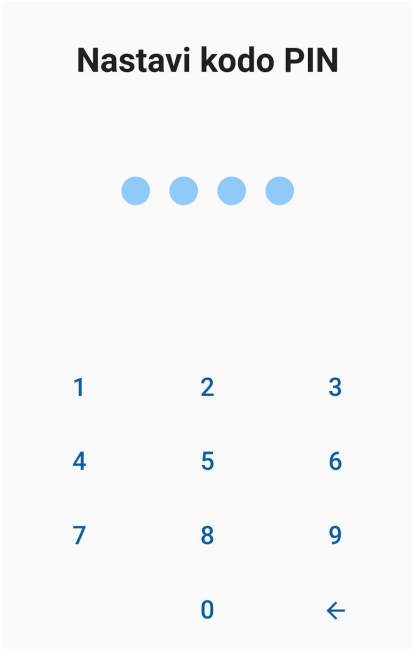
4. Po izvedeni dvofaktorski avtentikaciji se prikaže spodnji zaslon z napisom, da ste v postopku registracije svoje prve naprave.



5. Na naslednjem zaslonu morate poimenovati svojo napravo za njeno boljšo prepoznavo in upravljanje.

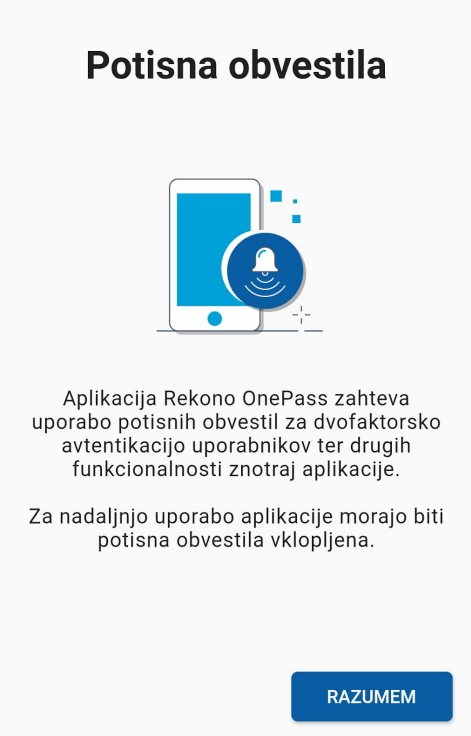


6. V naslednjem koraku nastavite svojo kodo PIN, ki bo v aplikaciji služila kot varnostni mehanizem.



7. Po nastavitvi in potrditvi vpisane kode PIN se prikaže zaslon, kjer lahko omogočite biometrično avtentikacijo, če jo vaša naprava podpira.

8. V naslednjem koraku aplikacija zahteva, da potrdite in omogočite (če niso že omogočena) obvestila v aplikaciji, ki so bistvenega pomena za potisna obvestila pri dvofaktorski prijavi.



9. Kliknite “**Razumem**”, da aplikacija vzpostavi začetno konfiguracijo in tako je naprava uspešno registrirana v vaš račun Rekono.

Potisna obvestila

Kaj so potisna obvestila?

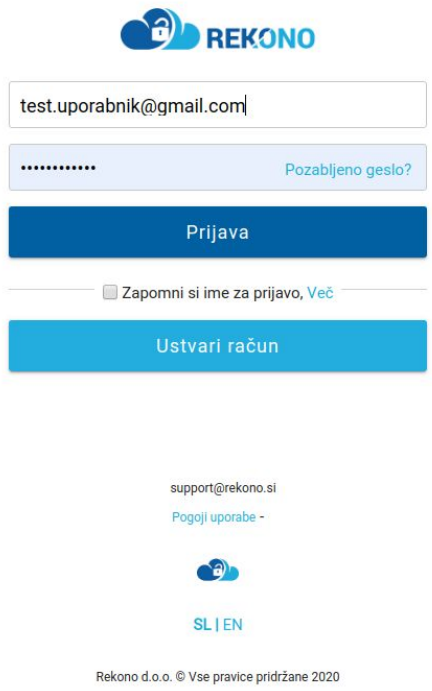
Potisna obvestila zagotavljajo hitrejšo in varnejšo prijavo z dvofaktorsko avtentikacijo na vaši napravi v primerjavi s katerimkoli drugim postopkom dvofaktorske avtentikacije. Ko uporabljate Rekono OnePass, morate obvezno **omogočiti obvestila za aplikacijo, drugače potisna obvestila za dvofaktorsko avtentikacijo ne bodo delovala**.

Kako se prijaviti v račun Rekono z uporabo potisnih obvestil?

Sledijo navodila za prijavo v račun Rekono z uporabo potisnih obvestil, ki imajo funkcijo mehanizma dvofaktorske avtentikacije.

Po registraciji svoje naprave v aplikaciji Rekono OnePass lahko uporabljate potisna obvestila kot mehanizem dvofaktorske avtentikacije. Upoštevajte spodnji postopek.

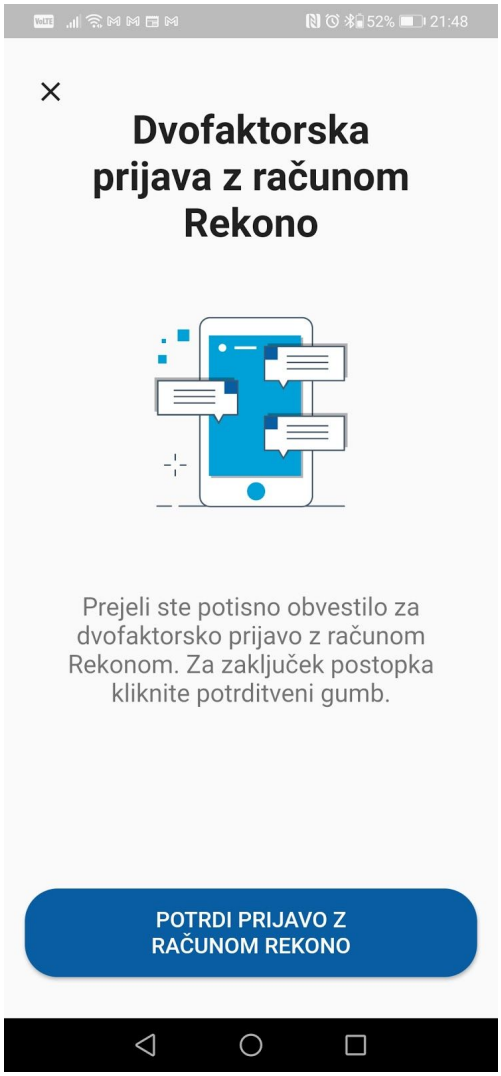
1. V brskalniku se prijavite v račun Rekono, tako da vpišete svoj e-naslov in geslo.



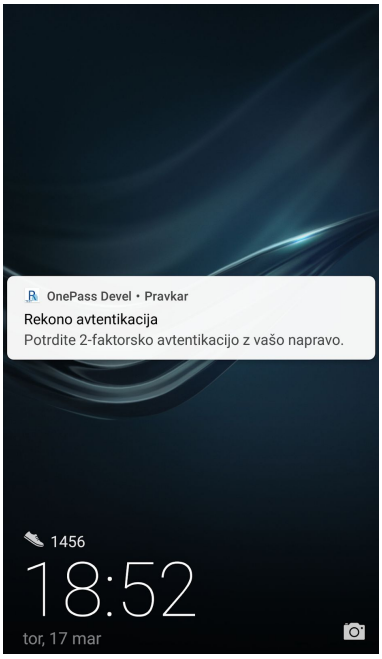
2. Svojo napravo ste registrirali, zato se med razpoložljivimi prijavnimi mehanizmi prikaže dvofaktorska avtentikacija s pomočjo potisnih obvestil. Izberite mehanizem **PRIJAVA ONEPASS**.

3. Na svojo napravo boste prejeli potisno obvestilo. Obstajata dva scenarija, kako aplikacija prejme potisna obvestila.

3a. Če vaša aplikacija Rekono OnePass že deluje, se vam bo takoj prikazal spodnji potrditveni zaslon.



3b. Če je aplikacija Rekono OnePass zaprta oziroma je naprava zaklenjena, prejmete na svojo napravo spodnje obvestilo.

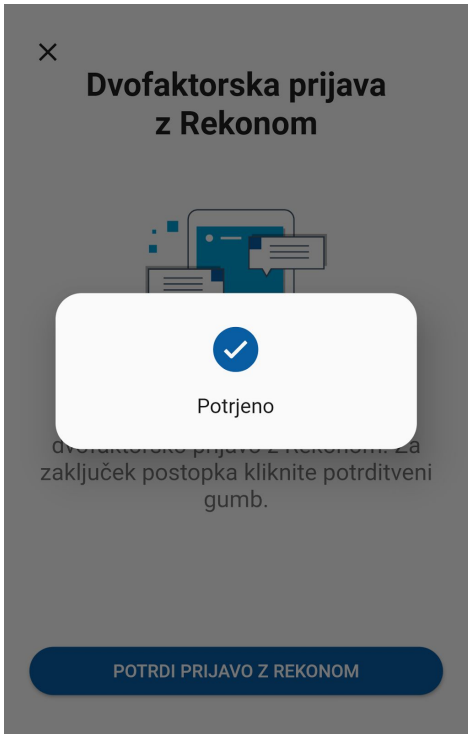


3b1. Kliknite obvestilo, ki samodejno odpre aplikacijo Rekono OnePass.

3b2. Prikaže se zaklenjeni zaslon, kjer za nadaljevanje uporabite biometrične podatke ali kodo PIN.

3b3. Po predstavitvi z biometričnimi podatki oziroma s kodo PIN na varnostnem zaslonu se prikaže zaslon za potrditev obvestila.

4. Kliknite gumb in potrdite, da ste prejeli potisno obvestilo.



5. Po potrditvi prejema potisnega obvestila bo sistem samodejno preveril vašo potrditev in preusmerjeni boste v nadzorno ploščo vašega računa Rekono.

Potrjevanje spletnih nakupov

Vpis s PIN/PAN

Aplikacija Rekono OnePass podpira potrjevanje spletnih nakupov, ki jih opravite s karticami vaših bank in njihovo povezavo s povezanim profilom Rekono.

Za aktiviranje vaše banke za spletne nakupe v aplikaciji Rekono OnePass potrebujete naslednje:

- Izbrano banko iz spustnega seznama bank.
- Zadnjih 6 številk PAN številke kreditne kartice.
- Davčno številko, ki mora biti identična tisti v vašem računu Rekono.
- V računu Rekono mora biti uporabljena enaka telefonska številka, kot ste jo sporočili svoji banki.
- Kodo PIN, povezano z vašo kreditno kartico.

Sledi postopek aktiviranja potrjevanja spletnih nakupov v aplikaciji Rekono OnePass z uporabo številke vaše kartice in kose PIN.
Pomembno: S pravilnim vnosom katerekoli kartice se aktivira potrjevanje spletnih nakupov vseh kartic izbrane banke, ki so povezane z vašo davčno številko.

1. Premaknite se na zavihek **Potrjevanje spletnih nakupov** v *Profilu Rekono* oz*. 3-D Secure* na spodnjem delu ekrana. Tu lahko upravljate banke, ki ste jih aktivirali v svojem račun. Za dodajanje banke kliknite ikono **Dodaj banko** v spodnjem desnem kotu zaslona.
2. Na naslednjem zaslonu morate vnesti prijavne podatke svoje bančne kartice. Izberite svojo **banko** v spustnem seznamu, vnesite **zadnjih 6 številk PAN številke svoje bančne kartice**, svojo **davčno številko,** če se ni že izpisala na zaslonu, ter ime imetnika bančne kartice. Kliknite **Nadaljuj**.
3. V kolikor so vsi podatki iz prejšnjega koraka pravilni, vnesite **kodo PIN** svoje bančne kartice ter kliknite **Preveri PIN** za preverjanje veljavnosti kode PIN na strežniku.
4. a. V kolikor ima vaš uporabniški račun **nivo zaupanja v e-identiteto nižji od 20 (srednji nivo)**, morate nadaljevati z dodatnim korakom vnosa osebnih podatkov v svoj račun Rekono. Preverite predizpolnjena polja in vpišite dodatne manjkajoče podatke. Ko so vsa polja pravilno izpolnjena, kliknite **Potrdi podatke**.
4. b. V kolikor ima vaš uporabniški račun že **nivo zaupanja v e-identiteto 20 (srednji nivo) ali višji** (torej je bil predhodno ustvarjen na preverjen način), ste dokončali postopek aktiviranja banke v svojem računu brez dodatnega vnosa osebnih podatkov. Izpiše se sporočilo, da je bila banka uspešno aktivirana v vašem računu Rekono.
5. Po potrditvi podatkov se izpiše sporočilo, da je bila banka uspešno aktivirana v vašem računu Rekono, dodana banka se prikaže na zaslonu za upravljanje bank.

Onemogočanje/odstranitev banke

Sledi kratko navodilo za odstranitev banke iz računa Rekono.

1. Premaknite se na zavihek **Potrjevanje spletnih nakupov** v *Profilu Rekono* oz. *3-D Secure* na spodnjem delu ekrana. Tu lahko upravljate banke, ki ste jih aktivirali v svojem računu. Za izbris izbrane banke kliknite ikono smetnjaka ob izbrani banki
2. V pojavnem oknu odgovorite na vprašanje, ali res želite izbrisati to banko iz svojega računa. Če potrdite, bo banka odstranjena iz vašega računa.
3. Za dezaktivacijo kliknite banko in jo nato z drsnikom onemogočite.

Potisna obvestila 3-D Secure

Kaj je 3-D Secure?

3-D Secure (3-domain structure) oziroma preverjanje istovetnosti (avtentikacija) plačnika je varnostni protokol, katerega namen je preprečevanje prevar pri spletnih plačilih s kreditnimi in debetnimi karticami. Ta dodatni varnostni standard sta ustvarili in vpeljali Visa in MasterCard kot svoji blagovni znamki ‘Verified by Visa’ in ‘MasterCard SecureCode’.

Integracija z aplikacijo Rekono OnePass

Aplikacija Rekono OnePass prejme zahtevo za transakcijo od trgovca v obliki potisnega obvestila 3-D Secure. Ko uporabnik prejme potisno obvestilo in se prijavi v aplikacijo Rekono OnePass s pomočjo biometrije ali kode PIN, se mora na prejeto obvestilo odzvati v 5 minutah v oknu za potrditev transakcije, ki se odpre po prejemu obvestila.

Sledi postopek transakcije s 3-D Secure v aplikaciji Rekono OnePass.

Postopek transakcije s 3-D Secure

1. Na svojo napravo prejmete potisno obvestilo 3-D Secure.
2. Vpišite svojo kodo PIN oziroma uporabite biometrično avtentikacijo za vpis v aplikacijo Rekono OnePass.
3. Preverite pravilnost podatkov o transakciji in potrdite plačilo, tako da kliknete **Potrdi plačilo**.

V primeru uspešne potrditve se odpre pojavno okno z obvestilom, da je bila potrditev transakcije 3-D Secure uspešna.

Podpisovanje dokumentov

Z aplikacijo Rekono OnePass lahko podpišete dokumente, ki ste jih shranili v svoji napravi, ali pa dokumente, ki ste jih prejeli s pomočjo razčlenjenega potisnega obvestila kot del postopka SCA (strogo preverjanje pristnosti stranke) podpisovanja dokumenta.

Sledi podroben opis postopka podpisovanja dokumentov z uporabo aplikacije Rekono OnePass.

Lokalno podpisovanje dokumentov

Z aplikacijo Rekono OnePass lahko podpišete dokumente, ki ste jih shranili v svoji napravi. Podpišete lahko katerikoli dokument, ki se nahaja v datotečnem sistemu vaše naprave. Ko je dokument uspešno podpisan, ga lahko delite v drugih aplikacijah ali storitvah za skupno rabo, ali pa ga prenesete v mapo z dokumenti v aplikaciji.

Sledi postopek podpisovanja lokalnega dokumenta.

1. Premaknite se na zavihek **Podpis Rekono** v aplikaciji Rekono OnePass in kliknite spodaj desno okrogel gumb, ki predstavlja dokument. Nato v shrambi svoje naprave izberite datoteko, ki jo želite podpisati.
2. Ko naložite dokument v aplikacijo, vas ta samodejno pozove, da podpišete naložen dokument.
3. Kliknite gumb za podpisovanje in začne se postopek podpisovanja dokumenta, kar je prikazano v pogovornem oknu.
4. Ko je dokument uspešno podpisan, ste preusmerjeni na zaslon s podpisanim dokumentom, kjer lahko upravljate podpisani dokument. Dokument lahko delite z drugimi aplikacijami ali storitvami, ali pa ga prenesete v svojo napravo.
5. Ko kliknete gumb za skupno rabo, se prikaže sistemsko pogovorno okno, ki je odvisno od operacijskega sistema vaše naprave.
6. Dokument lahko tudi shranite v shrambo naprave.

Podpisovanje dokumentov s pomočjo potisnih obvestil ob strogem preverjanju pristnosti uporabnika (postopek SCA)

Sledi postopek, v katerem s pomočjo potisnega obvestila podpišete dokumente in pridobite predogled dokumentov ob strogem preverjanju pristnosti uporabnika.

1. V svojo napravo prejmete potisno obvestilo.
2. Vpišite kodo PIN oziroma se avtenticirajte s pomočjo biometrije za vpis v aplikacijo.
3. Odpre se pojavno okno z vprašanjem, ali želite predogled podpisanih dokumentov oz. boste to storili kasneje.
4. Kliknite **Predoglej in podpiši**. V ozadju je v teku nalaganje nekaterih podatkov o dokumentih, kar se izpiše v pogovornem oknu.
5. Odpre se zaslon s predogledom podatkov predloge dokumentov, ki so v postopku podpisovanja.
   Na dnu zaslona se izpiše, kateri dokumenti so v postopku pridobitve in nalaganja.
6. Ko so vsi dokumenti naloženi, si lahko s klikom na gumb **Predogled** ogledate vsak dokument posebej, da zagotovite veljavnost dokumentov, ki so v postopku podpisovanja. Če želite podpisati izbrane dokumente, kliknite **Podpiši** na dnu okna, ali pa **Opusti**, če želite opustiti celoten postopek podpisovanja.
7. Ko kliknete **Podpiši**, se vam odpre okno z obvestilom, da so izbrani dokumenti v postopku podpisovanja.
8. Če je bilo podpisovanje uspešno, se to izpiše na zaslonu, kjer lahko dokumente tudi delite z drugimi aplikacijami (Google Drive, e-pošta, Cloud) ali pa jih shranite v svojo mobilno napravo.
9. a - Delite dokument z drugimi aplikacijami na svoji mobilni napravi.
   b - Shranite dokument v svojo mobilno napravo.

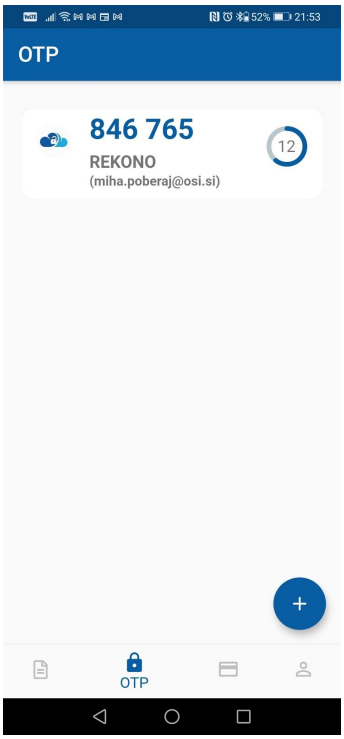
Uporaba enkratnih gesel OTP

Enkratno geslo OTP ima funkcijo močnega mehanizma dvofaktorske avtentikacije, ki ga je lahko vzdrževati, upravljati in dodati v aplikacijo Rekono OnePass. Enkratna gesla delujejo in so na voljo uporabniku celo brez aktivne internetne povezave (kar omejuje uporabo potisnih obvestil).

Samodejni vpis enkratnega gesla OTP aplikacije Rekono OnePass

Z registracijo naprave in prijavo v Rekono OnePass se v aplikacijo samodejno vpiše in shrani enkratno geslo OTP. To enkratno geslo zlahka vidite na glavnem navigacijskem zaslonu OTP aplikacije Rekono OnePass.

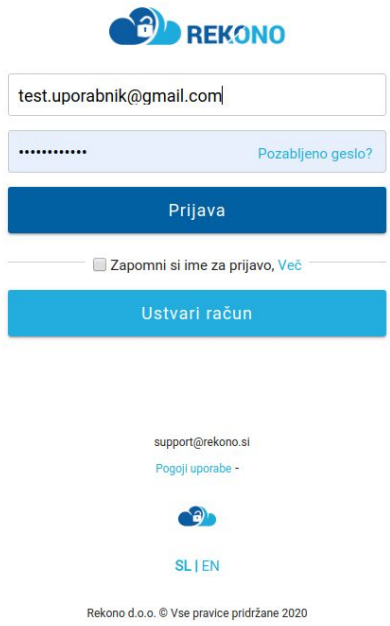
Enkratnega gesla aplikacije Rekono OnePass, ki se je samodejno vpisalo, **ne morete izbrisati,** saj opravlja funkcijo elementa dvofaktorske avtentikacije in mora biti zato izpisano na zaslonu OTP v aplikaciji. Uporabnik pa lahko poljubno preimenuje imenski identifikator enkratnega gesla.



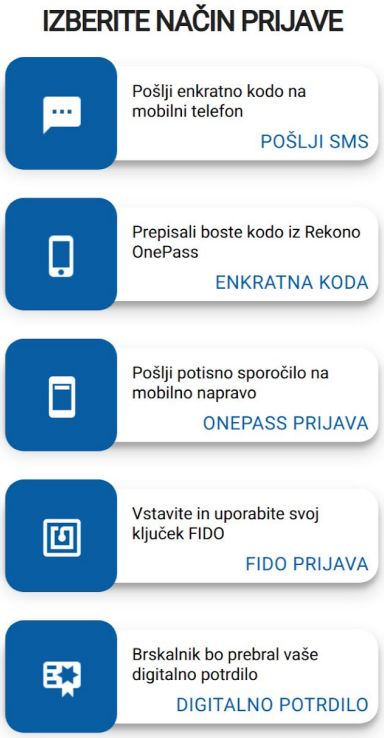
Kako se prijaviti v račun Rekono z uporabo enkratnega gesla OTP aplikacije Rekono OnePass?

Sledijo podrobna navodila za prijavo v račun Rekono z uporabo enkratnega gesla OTP, shranjenega v aplikaciji Rekono OnePass.

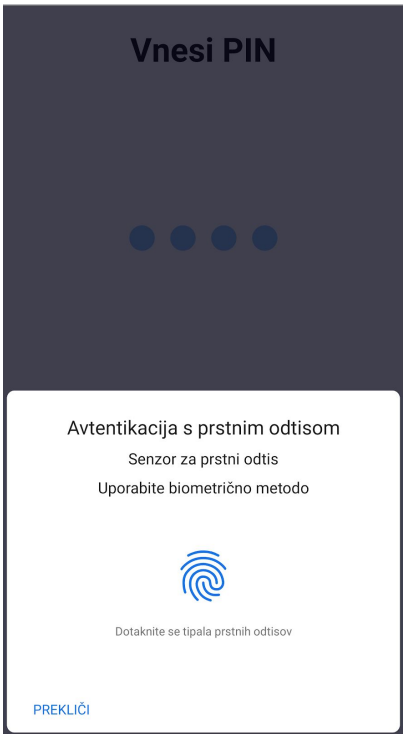
1. V brskalniku se prijavite v račun Rekono, tako da vpišete svoj e-naslov in geslo.



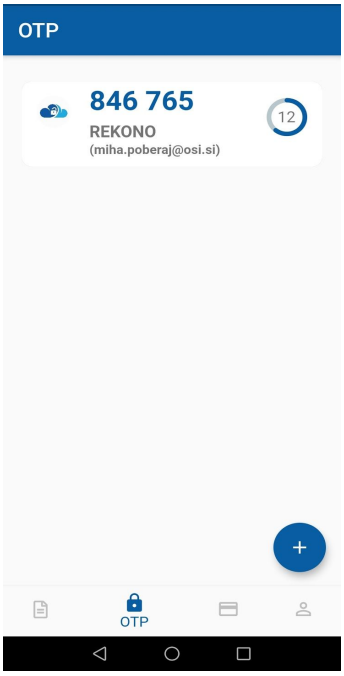
2. Izberite mehanizem dvofaktorske avtentikacije **ENKRATNO GESLO**.



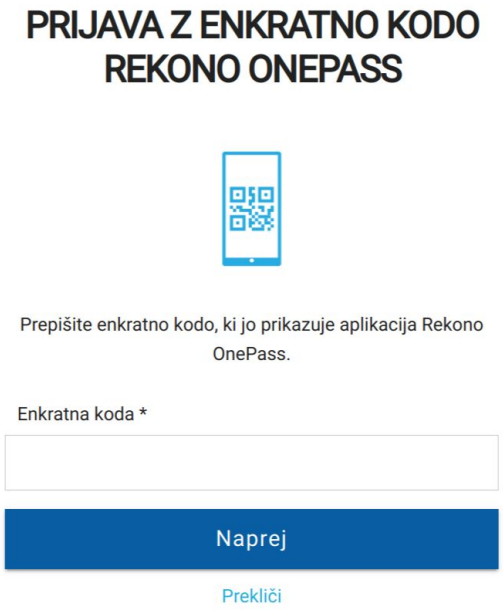
3. Odprite aplikacijo Rekono OnePass in na varnostnem zaslonu opravite avtentikacijo z biometričnimi podatki/kodo PIN.



4. Odpre se glavni zaslon OTP. Pazljivo kopirajte enkratno geslo iz aplikacije Rekono OnePass v polje v brskalniku.



5. Vnesite enkratno geslo, kopirano iz aplikacije Rekono OnePass, v predvideno polje in kliknite **Naprej.** S tem zaključite svojo prijavo v račun Rekono z dvofaktorsko avtentikacijo z enkratnim geslom.



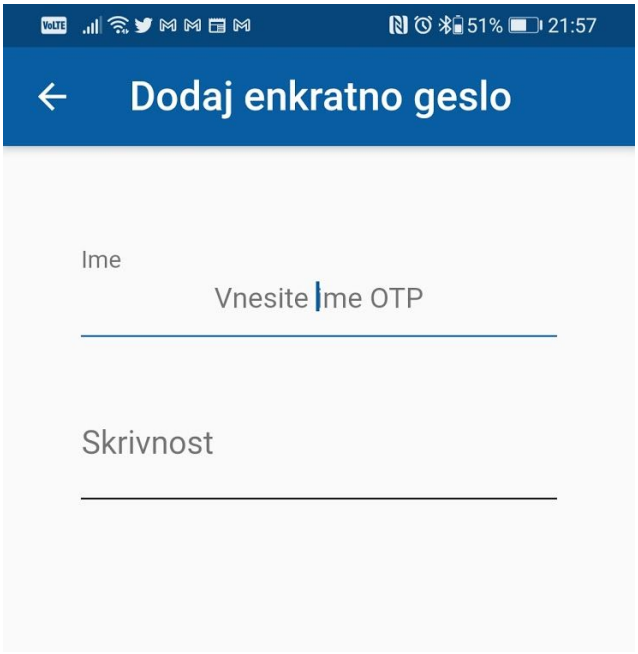
Kako dodati enkratno geslo v Rekono OnePass?

Novo enkratno geslo lahko v aplikacijo Rekono OnePass dodate na dva načina. Prvi način je s pomočjo ročnega vnosa, pri drugem načinu pa gre za samodejno skeniranje kode QR.

Ročno dodajanje enkratnega gesla

Novo enkratno geslo lahko ročno dodate v aplikacijo Rekono OnePass, tako da kliknete **Dodaj**, Prikažeta se možnosti **Skeniraj** ali **Vnesi** na glavnem navigacijskem zaslonu, kjer kliknete **Vnesi**.

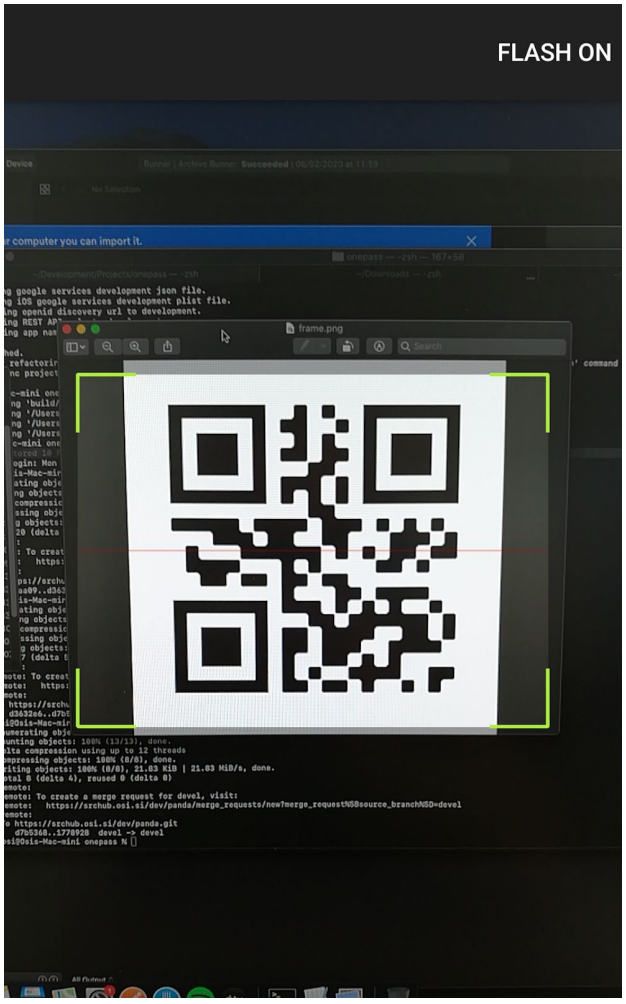
Nato vpišite svoje ime OTP, ki se bo izpisalo na glavnem zaslonu OTP, ter OTP skrivnost. Kliknite **Dodaj** za dodajanje enkratnega gesla OTP v svojo aplikacijo.



Samodejno dodajanje enkratnega gesla z vgrajenim bralnikom kode QR

Ta rešitev je precej hitrejša. Z uporabo fotoaparata na napravi in vgrajenega mehanizma za prepoznavo kode QR lahko hitro skenirate kodo QR, ki doda enkratno geslo v vašo aplikacijo.

Enkratno geslo dodate tako, da kliknete **Dodaj OTP** na glavnem navigacijskem zaslonu ter nato kliknete gumb za skeniranje. Pojavi se bralnik kode QR, s katerim skenirate želeno kodo. Koda QR je skenirana, njeni podatki pa so dodani v aplikacijo kot enkratno geslo.



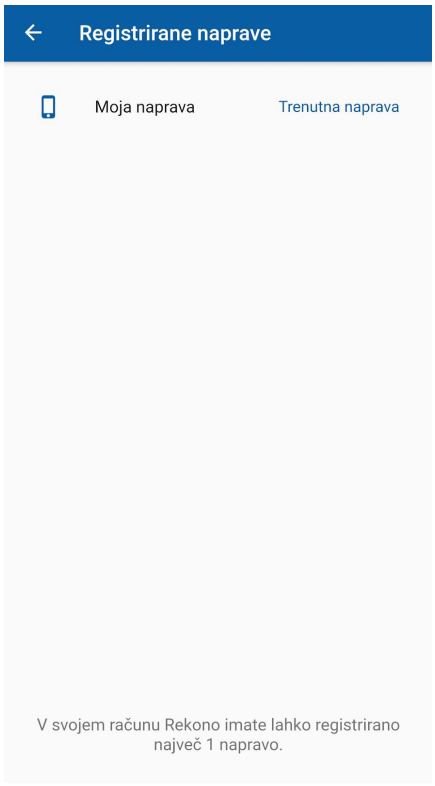
Upravljanje naprav

Upravljanje naprav je prav tako podprto v aplikaciji Rekono OnePass. Trenutno lahko v račun Rekono registrirate **največ eno napravo**, zato funkcionalnost upravljanja naprav v tem trenutku ni uporabna.

S prihodnjimi posodobitvami pa boste lahko v račun Rekono registrirali dve napravi, od tega bo imela vsaka naprava shranjeno v aplikaciji Rekono OnePass svoje enkratno geslo, ime, preference in nastavitve.

Prikaz naprav v aplikaciji Rekono OnePass

Vidite lahko vse naprave, ki so registrirane v aplikaciji Rekono OnePass. Kliknite sklop **Vse naprave** v razdelku *Naprave*. Desno od imena naprave, ki je trenutno v uporabi, je to izpisano z modrimi črkami “**Trenutna naprava**”, da uporabnik ve, katera naprava je trenutno v uporabi.



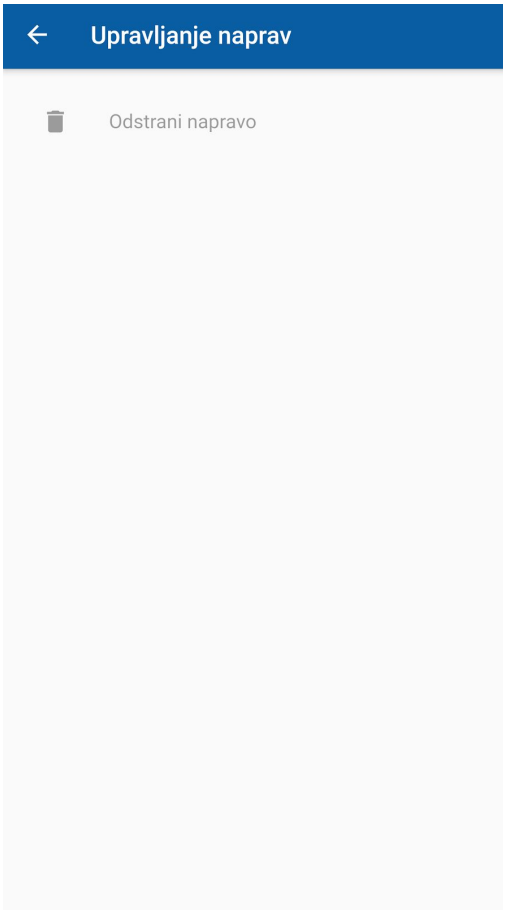
Kako odstraniti napravo iz računa Rekono?

Za odstranitev naprave iz računa Rekono sta na voljo dve možnosti, in sicer odstranitev notranje naprave ter odstranitev zunanje naprave.

Odstranitev notranje naprave (implementirano v prihodnji posodobitvi)

Odstranitev notranje naprave pomeni, da lahko uporabnik, ki ima v svojem računu Rekono registrirano več kot eno napravo, odstrani določeno napravo v aplikaciji Rekono OnePass.

Funkcionalnost pride prav v primerih, ko izgubite drugo napravo ali pa je ne morete odkleniti ter želite preprečiti, da bi kdo drug zlorabil vašo napravo ter se prijavil v Rekono OnePass in ukradel pomembne podatke. V razdelku za upravljanje zlahka odstranite izbrano napravo iz svojega računa, pri tem pa ni potreben dodaten varnostni element.



Odstranitev zunanje naprave

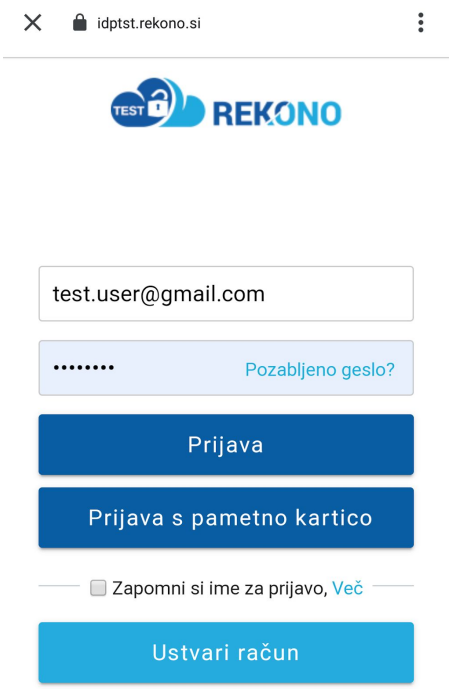
Postopek odstranitve zunanje naprave uporabite, ko izgubite aktivno napravo, je ne morete odkleniti ali pa se morate prijaviti v aplikacijo Rekono OnePass in registrirati novo napravo, pri tem pa nimate možnosti, da bi staro/izgubljeno napravo izbrisali.

Med postopkom odstranitve zunanje naprave morate uporabiti **kodo PUK**, povezano z vašim računom Rekono. To nudi dodatno varnost pri upravljanju naprave in zagotavlja, da lahko samo vi upravljate odstranitev zunanje naprave, saj samo vi poznate kodo PUK, ki je vaša last.

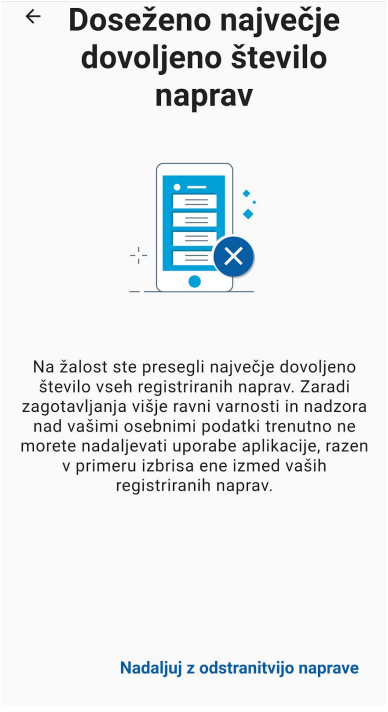
Sledi podrobno navodilo za odstranitev zunanje naprave z uporabo kode PUK.

1. V račun Rekono hočete dodati novo napravo, zato na napravo namestite aplikacijo Rekono OnePass in začnite postopek prijave.

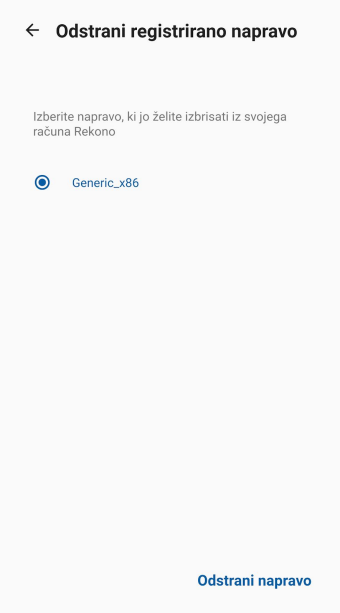
2. V aplikaciji Rekono OnePass se prijavite v račun Rekono s svojimi prijavnimi podatki.



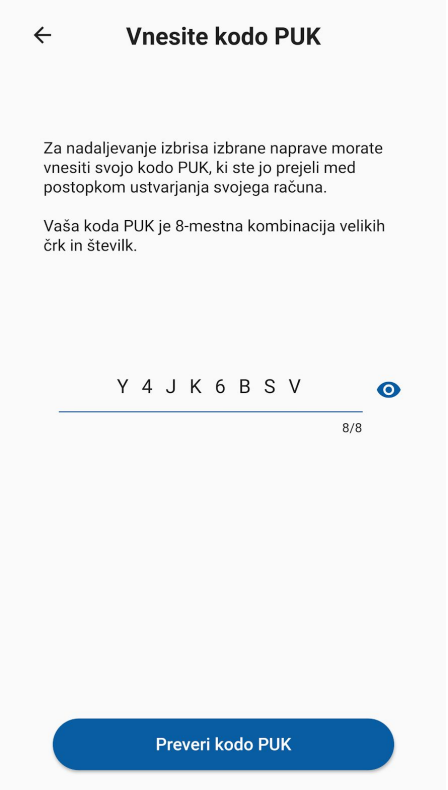
3. Ko uspešno opravite dvofaktorsko avtentikacijo, se prijavite v aplikacijo Rekono OnePass, kjer se vam na zaslonu izpiše, da ste dosegli omejitev glede števila naprav, prijavljenih v račun Rekono. Če želite nadaljevati, morate odstraniti eno od prejšnjih naprav.



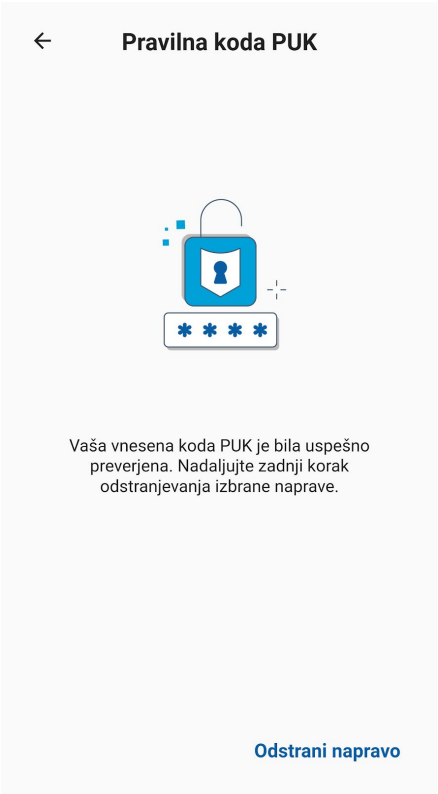
4. Na naslednjem zaslonu se izpiše seznam naprav, kjer izberete tisto, ki jo želite odstraniti. Če v svoj račun niste vpisali kode PUK, ne morete nadaljevati, zato poskrbite, da boste kodo PUK povezali s svojim računom Rekono.



5. Ko izberete napravo, ki jo želite odstraniti, vpišite **kodo PUK**, povezano z vašim računom Rekono, ki ste jo shranili na varnem mestu in jo poznate samo vi.



6. V naslednjem koraku aplikacija preveri, ali je vpisana koda PUK pravilna. Če ste vnesli veljavno kodo PUK, lahko dokončate postopek odstranitve svoje naprave iz računa Rekono, tako da kliknete **Odstrani napravo**.



7. Postopek odstranitve zunanje naprave je zaključen, zdaj pa imate možnost, da dodate in registrirate novo napravo v račun Rekono.

Varnost

Varnostne značilnosti

Zaščita pred obratnim inženirstvom

Aplikacija OnePass je zaščitena s številnimi varnostnimi postopki, ki preprečujejo in zmanjšujejo tveganje, da bi napadalec s pomočjo obratnega inženirstva skušal priti do skrivnosti aplikacije in žetonov. Zaradi uporabe obfuskacije in optimizacije kode ter krčenja kode in virov sta napadalcu interpretacija in obratno inženirstvo aplikacije precej otežena. Z obfuskacijo skrajšamo in zmanjšamo razrede, metode in imena spremenljivk, da obratno inženirstvo tako rekoč ni mogoče zaradi neberljive kode in konfiguracijskih datotek.

Zaradi krčenja kode in virov, s pomočjo katerega varno odstranimo neuporabljene razrede, polja, metode in atribute ter neuporabljene vire v aplikaciji ter odvisnosti knjižnic, se velikost aplikacije precej zmanjša, kar je v prid tudi njeni učinkovitosti delovanja.

POMEMBNO: Ne pozabite, da ne obstaja stoodstotno varna metoda, ki lahko v celoti prepreči napade obratnega inženirstva na vašo aplikacijo. S tem postopkom kodo samo spravimo v za človeka neberljiv format, zato napadalci težko pridejo do skrivnosti v vaši aplikaciji.

Varnostni elementi znotraj aplikacije

Notranja varnost aplikacije temelji na zaklenjenem zaslonu, ki vsebuje kodo PIN in biometrično avtentikacijo za naprave, ki to podpirajo. To zagotavlja zaupanja vreden in varen vstop v aplikacijo. Ob uporabi Rekono OnePass se pri vsaki ključni varnostni izpostavljenosti prikaže varnostni zaklenjeni zaslon, ki preprečuje kakršnokoli zlorabo aplikacije oziroma pomembnih podatkov uporabnika.

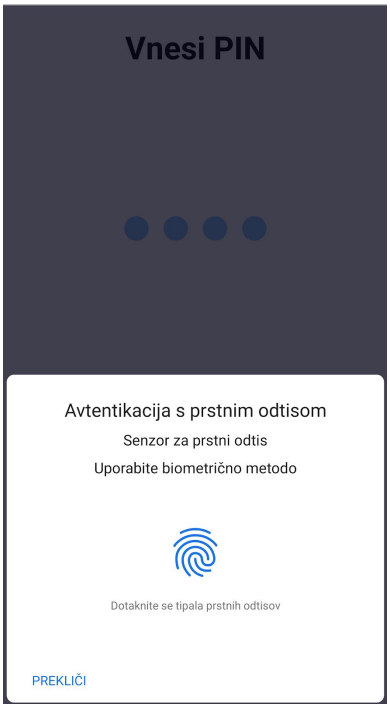
Biometrična avtentikacija

Biometrična varnostna podpora je glavna značilnost notranje varnosti aplikacije. Pri operacijskem sistemu Android je na voljo biometrična avtentikacija s pomočjo **PRSTNEGA ODTISA**, pri operacijskem sistemu iOS pa sta na voljo možnosti **ID OBRAZA** (FACE ID) in **PRSTNEGA ODTISA** (Apple TOUCH ID).

Z uporabo biometrične avtentikacije je interakcija uporabnika z aplikacijo hitrejša, kar omogoča nemoteno in uporabniku prijazno uporabo aplikacije.

Biometrično podporo lahko omogočite/onemogočite pri uvodnih nastavitvah aplikacije ali kasneje v nastavitvah v aplikaciji.

Primer biometričnega varnostnega zaklenjenega zaslona:



Varnostni element kode PIN

Notranja koda PIN je še vedno primarni notranji varnostni element zaklepanja. Prikazana je pod biometričnim pozivnim oknom (če jo naprava podpira).

Z varnostnim elementom kode PIN nudi aplikacija močno avtentikacijo za starejše naprave, ki nimajo integriranih biometričnih elementov.
Ko je koda PIN nastavljena, je varno shranjena v lokalnem prostoru za shranjevanje v aplikaciji z uporabo Keystore (Android)/Keychain (iOS) in varno šifrirana z uporabo šifriranja AES.

Prva nastavitev kode PIN

Kodo PIN nastavite med postopkom uvodne nastavitve aplikacije, ko registrirate svojo napravo v račun Rekono. Kodo PIN vpišete in jo potrdite na naslednjem zaslonu.

Spreminjanje kode PIN

Po prijavi v aplikacijo Rekono OnePass lahko kadarkoli spremenite svojo kodo PIN. Staro kodo PIN morate poznati, saj jo boste morali vpisati med postopkom spremembe kode PIN.

Postopek za spremembo kode PIN za dostop v aplikacijo je naslednji:

1. Kliknite **Spremeni kodo PIN** v varnostnem razdelku aplikacije.
2. Vpišite staro kodo PIN.
3. Vpišite novo kodo PIN.
4. S ponovnim vnosom potrdite novo kodo PIN.
5. Koda PIN je bila uspešno spremenjena.

Omejitve kode PIN

Ob vnosu kode PIN za avtentikacijo imate na voljo 3 poskuse za pravilen vpis kode PIN. Če niste uspešni, vam aplikacija onemogoči vstop v aplikacijo za 90 sekund.

Zaklenjen zaslon v primeru nedejavnosti

Kaj pomeni zaklenjen zaslon v primeru nedejavnosti?

Ker hočemo, da je aplikacija ves čas varna, tudi če niste omogočili zaklepanja zaslona v primeru nedejavnosti v sistemu svoje naprave, ima aplikacija integriran lastni zaklep zaslona v primeru nedejavnosti.

Zaklenjeni zaslon se prikaže, ko nekaj časa niste bili dejavni v aplikaciji (če ste pozabili zapreti aplikacijo oziroma niste omogočili zaklenjenega zaslona v sistemu naprave in ste pustili svojo napravo brez nadzora).

Po tem časovnem intervalu se zaradi nedejavnosti prikaže PIN/biometrični zaklenjeni zaslon. Ob namestitvi aplikacije je časovni interval privzeto nastavljen na 3 minute, toda to lahko prilagodite v nastavitvah glede na svoje potrebe.

Preklop med aplikacijami v ozadju

Če preklapljate med aplikacijami na svoji napravi in gre Rekono OnePass v način delovanja v ozadju, potem pa se vrnete nazaj v aplikacijo Rekono OnePass, se vam v aplikaciji prikaže samodejni varnostni zaklenjeni zaslon, ki preprečuje zlorabo in napačno uporabo aplikacije.

Analitika in poročanje o napakah

Rekono OnePass uporablja analitiko Firebase in njene druge storitve za zagotavljanje ustrezne dnevne analize odzivanja aplikacije in splošnega delovanja. Uporaba analitike, ki vključuje spremljanje dnevnih poročil in statistik uporabnikov, nam omogoča izboljšanje aplikacije.

Poročanje o napakah

Za čim boljšo uporabo aplikacije ter nemoteno in udobno izkušnjo uporabljamo analitiko, s pomočjo katere zaznavamo napake, ki se pojavljajo v aplikaciji, in jih tako tudi bolje organiziramo.

Močno **priporočamo,** da v aplikaciji Rekono OnePass omogočite poročanje o napakah, saj bomo tako lažje izboljšali uporabniško izkušnjo in delovanje funkcionalnosti.

Poročanje o napakah lahko vklopite v zavihku **Napredne nastavitve**.

Podpora različic operacijskega sistema

Platforma Android

Aplikacija podpira naprave na platformi Android z operacijskim sistemom različica **4.4 (Kitkat - API level 19)** in višje.

Platforma iOS

Aplikacija podpira naprave na platformi iOS z operacijskim sistemom različica **10.0** in višje.