ASA BANKA
Naša i snažna!

M-token

Korisničko uputstvo

Sadržaj

1. Uvod

ASA Banka mToken predstavlja funkcionalnost unutar mBanking aplikacije koja se koristi za sigurnu identifikaciju korisnika prilikom prijave u elektronsko bankarstvo, kao i za autorizaciju transakcija.

Za inicijalnu aktivaciju potreban je pristup internetu, dok se daljnje korištenje može odvijati i bez aktivne mrežne konekcije.

U slučaju promjene ili gubitka mobilnog uređaja, korisnik je dužan kontaktirati najbližu poslovnicu Banke.

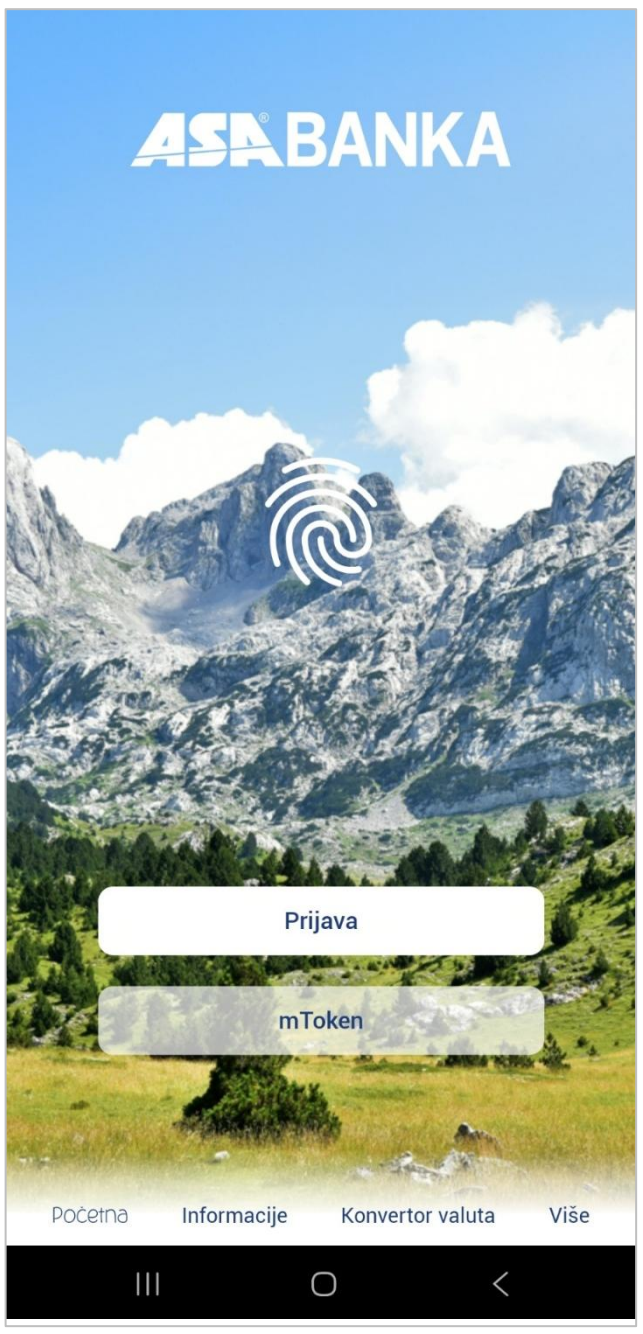
2. Pokretanje mToken funkcionalnosti

Nakon instalacije i otvaranja mBanking aplikacije, korisnik pristupa mToken funkcionalnosti odabirom „mToken" iz izbornog menija.

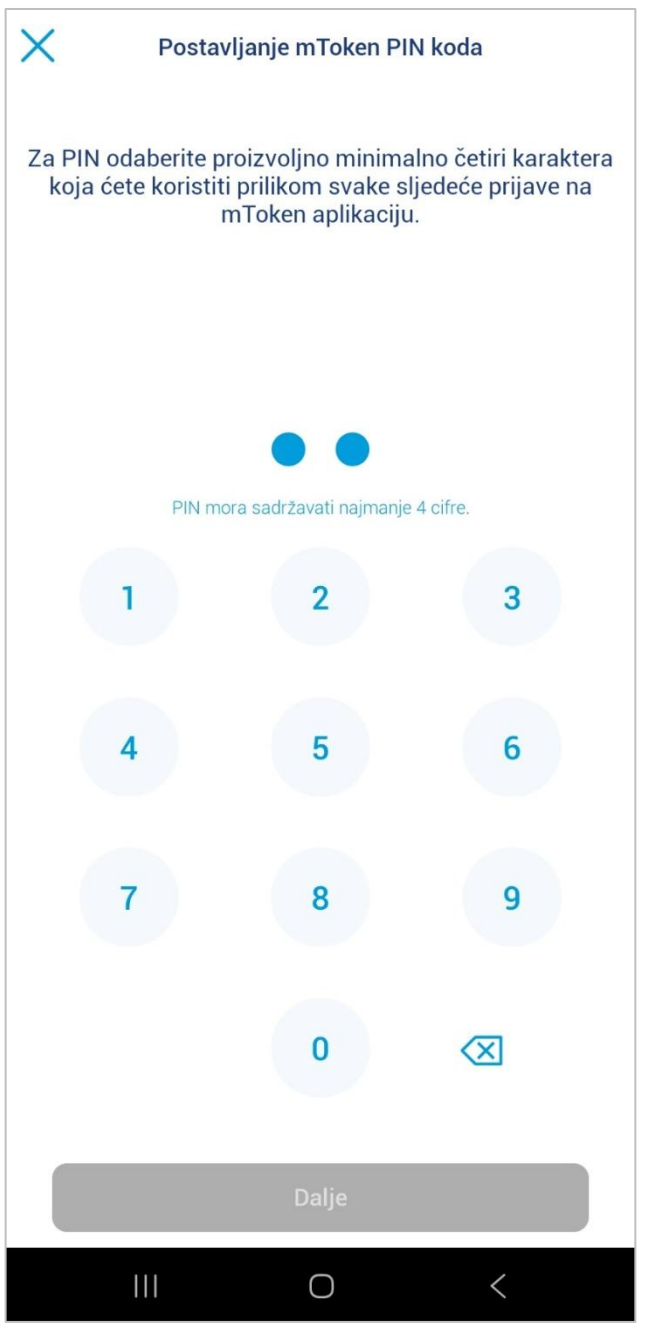
3. Definisanje PIN vrijednosti

Prvi korak pri korištenju mToken funkcionalnosti je definisanje PIN-a.
Korisnik unosi željeni PIN i zatim ga potvrđuje ponovnim unosom iste vrijednosti.

PIN mora sadržavati najmanje 4 karaktera i koristi se pri svakom narednom pristupu mToken funkcionalnosti. Preporučuje se izbjegavanje jednostavnih i lako prepoznatljivih kombinacija, kao što su uzastopni brojevi ili datumi rođenja. PIN treba biti poznat isključivo korisniku i ne treba ga zapisivati niti čuvati na uređaju. Ako korisnik tri puta uzastopno unese pogrešan PIN, mToken funkcionalnost se trajno onemogućava i za ponovno korištenje potrebno je obratiti se banci radi izdavanja novih aktivacijskih podataka.



Slika 1 – Izborni meni mBanking aplikacije

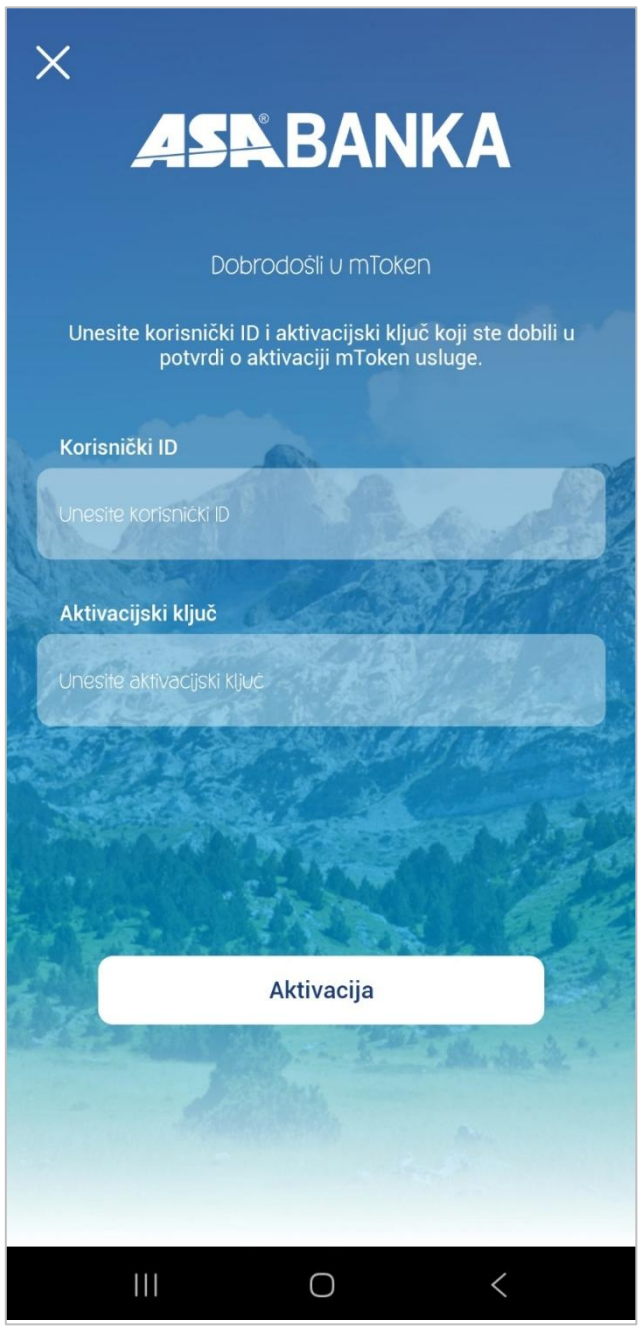


Slika 2 – Postavljanje PIN koda

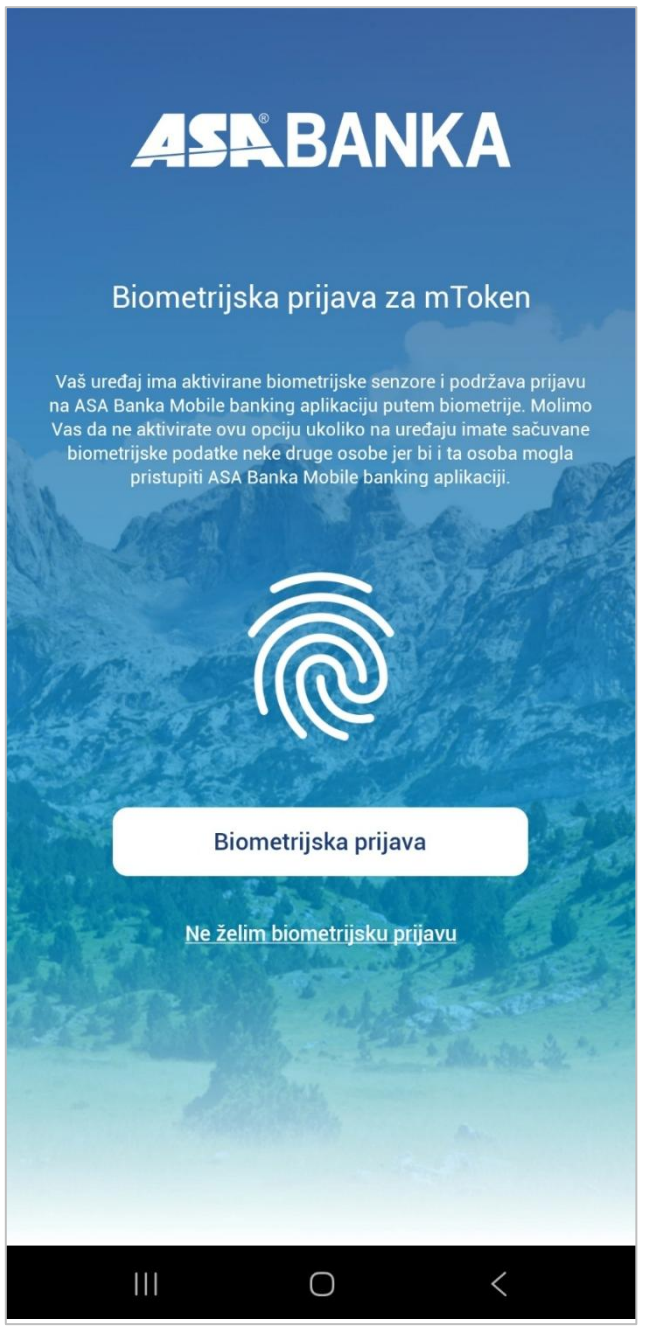
4. Aktivacija mToken funkcionalnosti

Nakon definisanja PIN-a, potrebno je izvršiti aktivaciju unosom korisničkog ID-a i aktivacijskog ključa koji ste prethodno dobili putem SMS-a. Ovi podaci koriste se samo prilikom prvog pokretanja i vremenski su ograničeni. Nakon njihovog unosa, korisnik potvrđuje prijavu, čime se mToken funkcionalnost aktivira i povezuje sa njegovim korisničkim podacima.

Po završetku aktivacije, korisniku može biti omogućeno uključivanje biometrijske prijave (otisak prsta ili prepoznavanje lica), u zavisnosti od podrške uređaja, čime se dodatno pojednostavljuje i ubrzava pristup mToken funkcionalnosti.



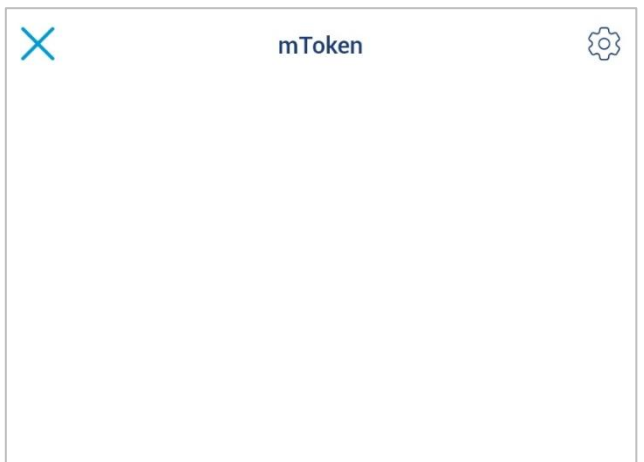
Slika 3 – Aktivacija mToken



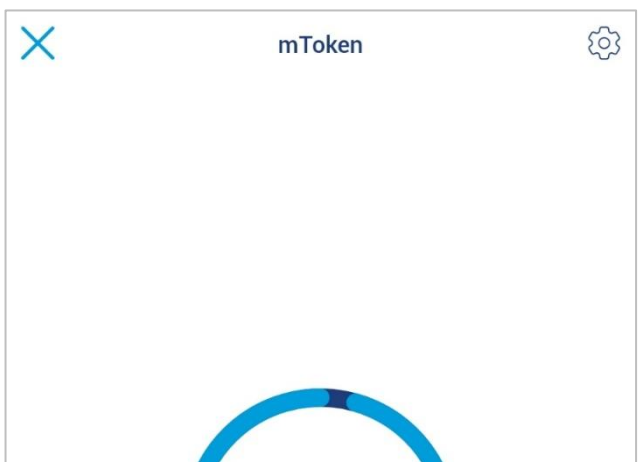
Slika 4 – Biometrijska prijava

5. Generisanje jednokratne lozinke (OTP)

Odabirom opcije za generisanje jednokratne lozinke, aplikacija prikazuje sigurnosni kod zajedno sa vremenom njegovog važenja. Korisnik taj kod unosi u odgovarajuće polje u elektronskom bankarstvu, pri prijavi ili potvrdi naloga. Kod se može iskoristiti samo jednom i važi ograničeno vrijeme, nakon čega je potrebno generisati novi. Ova metoda je jednostavna za korištenje jer se kod dobija jednim izborom opcije unutar aplikacije.



Slika 5 – Generisanje koda



Slika 6 – OTP broj

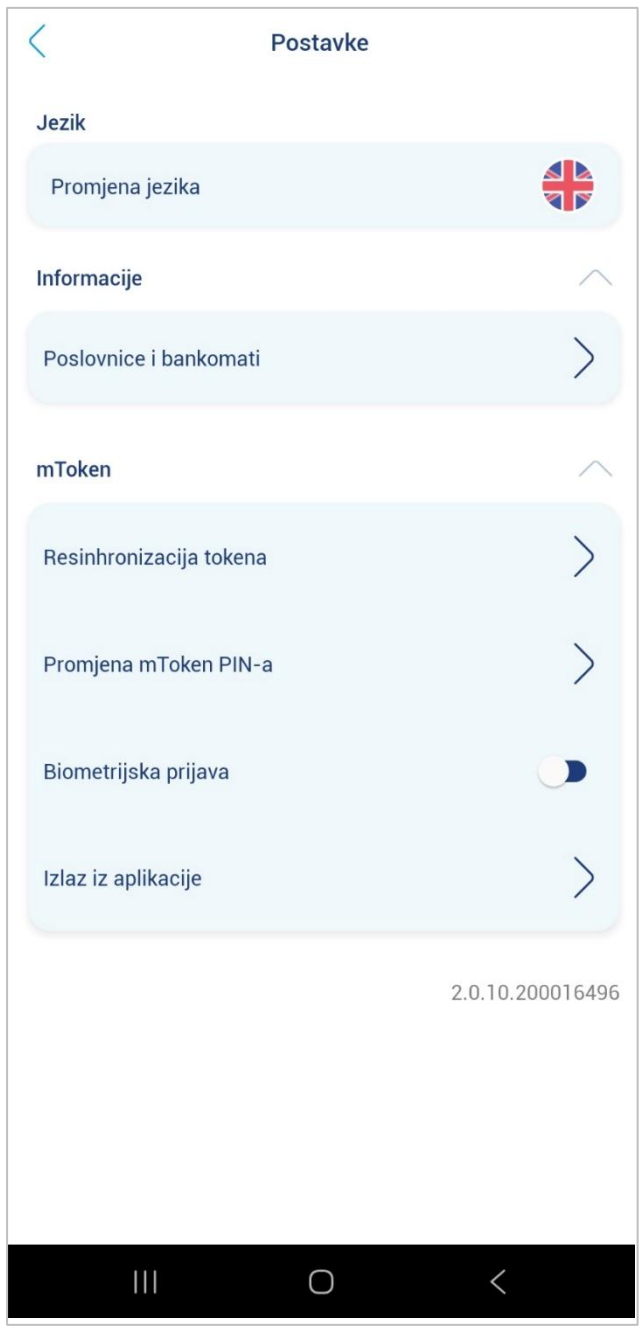
6. Dodatne opcije i postavke

Odabirom ikonice za postavke, otvara se izborni meni sa dodatnim opcijama funkcionalnosti.

Iz ovog izbornika moguće je:

- Promijeniti jezik mToken aplikacije odabirom opcije „Promjena jezika" – izmjena jezika vrši se automatski nakon klika na sličicu zastave
- Pretražiti bankomate i poslovnice Banke
- Uraditi resinhronizacija tokena (Idi na 6.1. Resinhronizacija tokena)
- Promijeniti PIN kod za mToken (Idi na 6.2. Promjena PIN koda)
- Omogućiti / onemogućiti biometrijsku prijavu na mToken
- Zatvoriti mToken (vratiti se na početni izborni meni mBanking aplikacije)

Na dnu izbornika nalazi se oznaka verzije aplikacije.



Slika 7 – Postavke i dodatne opcije

6.1. Resinhronizacija mTokena

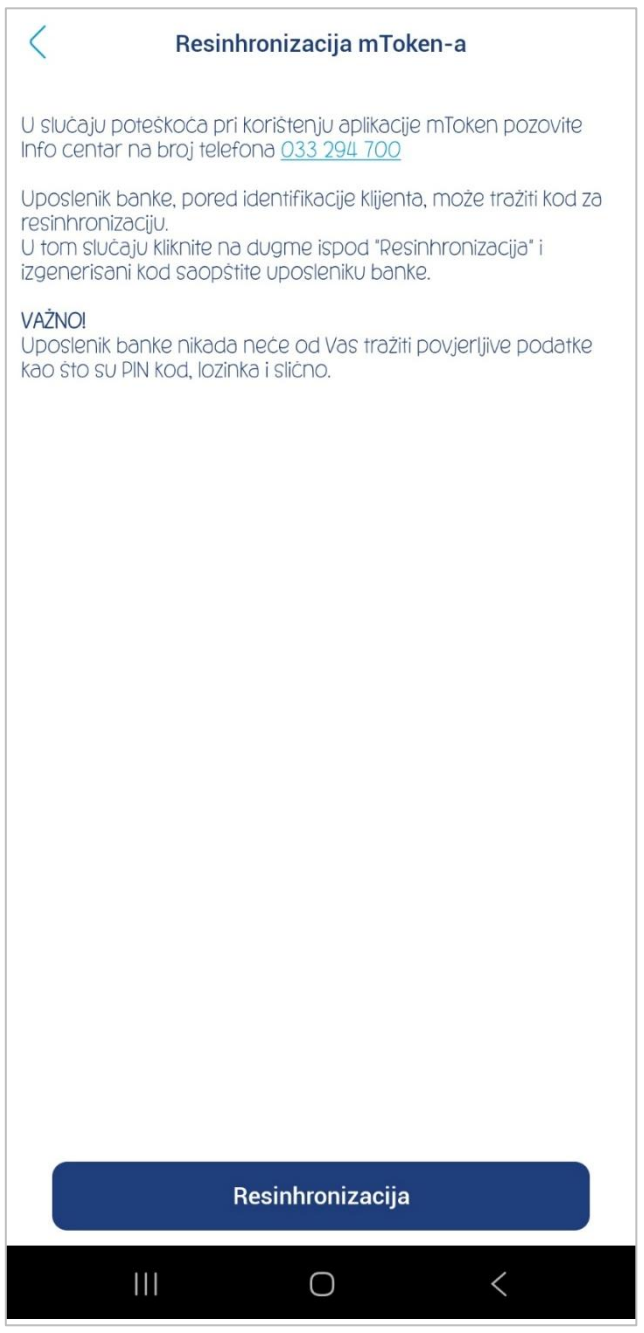
U slučaju poteškoća u radu mToken funkcionalnosti (npr. neispravni kodovi, odbijanje autentikacije ili nemogućnost prijave), može biti potrebno izvršiti resinhronizaciju. Ova procedura se koristi za ponovno usklađivanje mToken funkcionalnosti sa bankarskim sistemom.

Resinhronizaciju nije moguće izvršiti samostalno bez podrške banke. Prije pokretanja postupka, korisnik je dužan kontaktirati banku putem dostupnih kontakt kanala i izvršiti proces identifikacije prema uputama banke.

Nakon uspješne identifikacije, korisnik unutar mToken funkcionalnosti pomoću opcije „postavke" bira opciju **„Resinhronizacija"**. Aplikacija će tada generisati jedinstveni resinhronizacijski ključ koji se prikazuje na ekranu.

Korisnik je obavezan da prikazani ključ saopšti uposleniku banke, nakon čega banka vrši potrebne radnje za ponovno usklađivanje sistema. Po završetku procesa, mToken funkcionalnost će ponovo biti spremna za korištenje.

Važno je naglasiti da banka od korisnika nikada neće tražiti povjerljive podatke kao što su PIN, lozinka ili drugi sigurnosni podaci. Tokom procesa resinhronizacije dijeli se isključivo generisani ključ prikazan unutar aplikacije.



Slika 8 – Resinhronizacija upute za dalje postupanje

Slika 9 – Ključ za resinhronizaciju

6.2. Promjena PIN koda

Korisnik može u bilo kojem trenutku promijeniti PIN unutar mToken funkcionalnosti u mBanking aplikaciji, ukoliko smatra da je sigurnost kompromitovana ili želi koristiti novu kombinaciju.

Promjena PIN-a vrši se kroz postavke mToken funkcionalnosti odabirom opcije **„Promjena PIN-a"**.

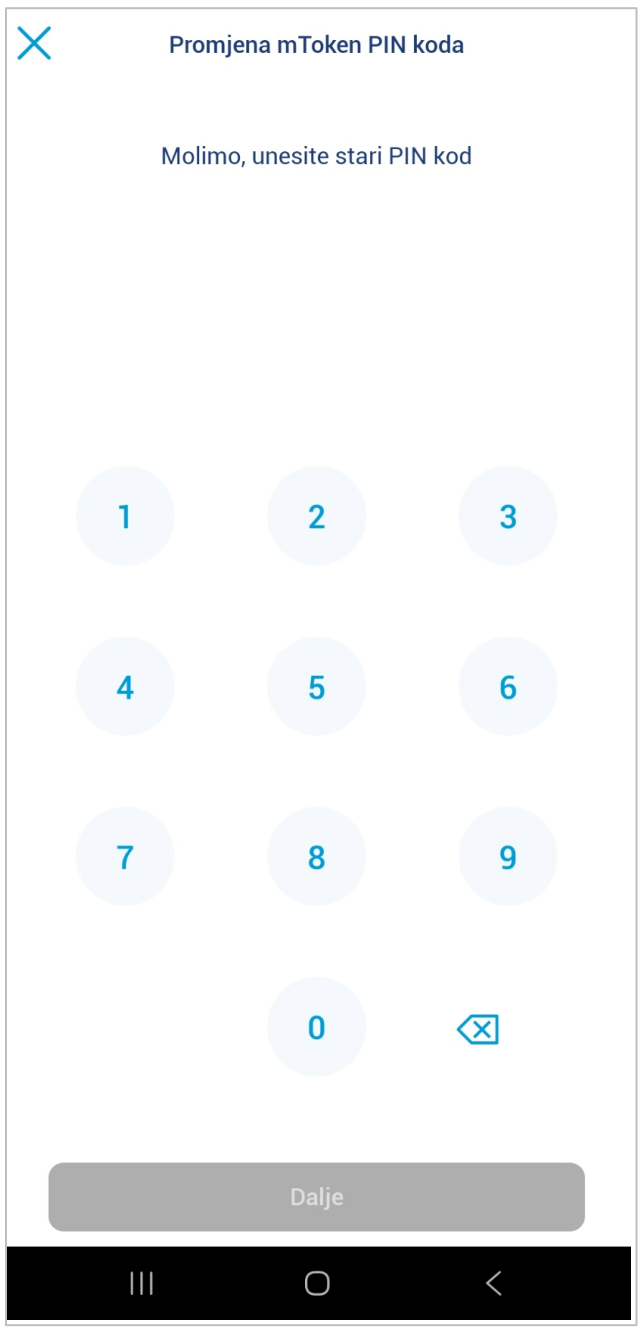
Za uspješnu promjenu potrebno je:

- unijeti trenutno važeći PIN
- unijeti novi PIN
- potvrditi novi PIN ponovnim unosom

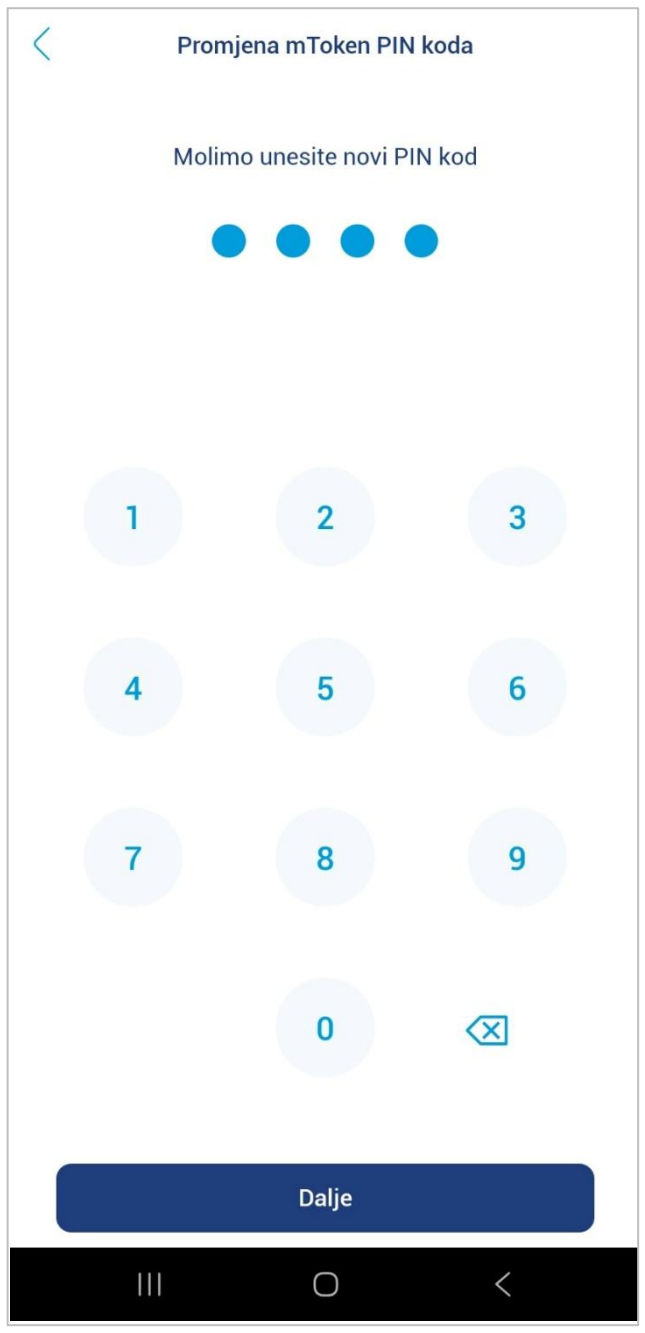
Novi PIN mora sadržavati najmanje 4 karaktera. Preporučuje se korištenje kombinacije koja nije lako predvidiva, te izbjegavanje jednostavnih nizova i ličnih podataka.

U slučaju da uneseni trenutni PIN nije ispravan, aplikacija će prikazati poruku o grešci i promjena neće biti izvršena. Ukoliko korisnik više puta unese pogrešan PIN i prekorači dozvoljeni broj pokušaja, pristup mToken funkcionalnosti može biti onemogućen, te je potrebno kontaktirati banku radi ponovne aktivacije.

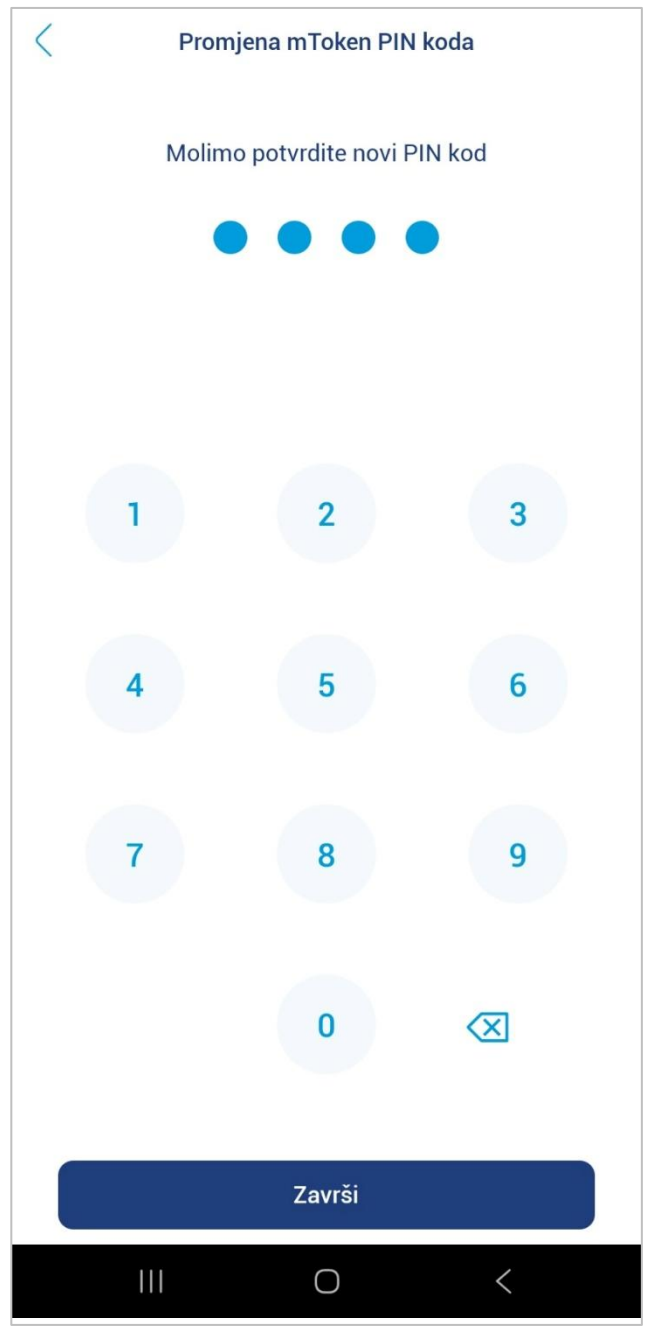
PIN je povjerljiv podatak i treba biti poznat isključivo korisniku. Ne preporučuje se njegovo zapisivanje niti dijeljenje sa drugim osobama.



Slika 10 – Unos trenutno važećeg PIN-a



Slika 11 – Unos novog PIN-a



Slika 12 – Potvrda novog PIN-a