

UPUTSTVO ZA KORIŠTENJE TOKENA I BITNE INFORMACIJE ZA POSLOVNE SUBJEKTE ZA USLUGU NETBANKING/MBANKING

1. Korištenje TOKEN-a prilikom pokretanja netBanking aplikacije

U nastavku Uputstva možete pronaći osnovne informacije bitne za: korištenje tokena, izvršenje plaćanja putem elektronskog bankarstva, kao i ostale bitne informacije koje se tiču sigurnosti Vašeg računa.

Ukoliko ste izabrali mToken, **mToken Sparkasse** aplikaciju prethodno trebate preuzeti putem oficijelnih trgovina aplikacija (Google Play Store, Apple Store). Za detaljno korištenje mToken-a molimo Vas da pogledate posebno uputstvo za korištenje mToken-a dostupno na Internet stranici banke.

Uputstvo za korištenje tokena kao i sva ostala Uputstva za korištenje aplikacije netBanking/mbanking su dostupna na Internet stranici <https://www.sparkasse.ba/bs/pravna-lica/e-bankarstvo/netbanking>.

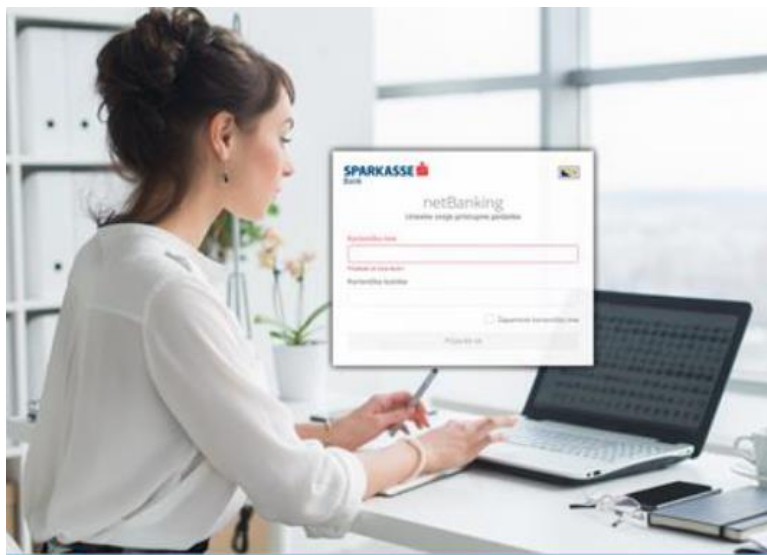
Token je uređaj, namijenjen identifikaciji korisnika internet bankarstva i digitalnom potpisivanju naloga tako da ne postoji mogućnost neovlaštenog pristupa klijentovim računima.

Za sva pitanja i probleme prilikom korištenja aplikacije molimo Vas da se obratite Banci putem Info linije na broj +387/33/280-300 i/ili na e-mail adresu netbanking.pl@sparkasse.ba i/ili nadležnom Voditelju poslovnog odnosa.

Pokretanje i prijava na aplikaciju netBanking

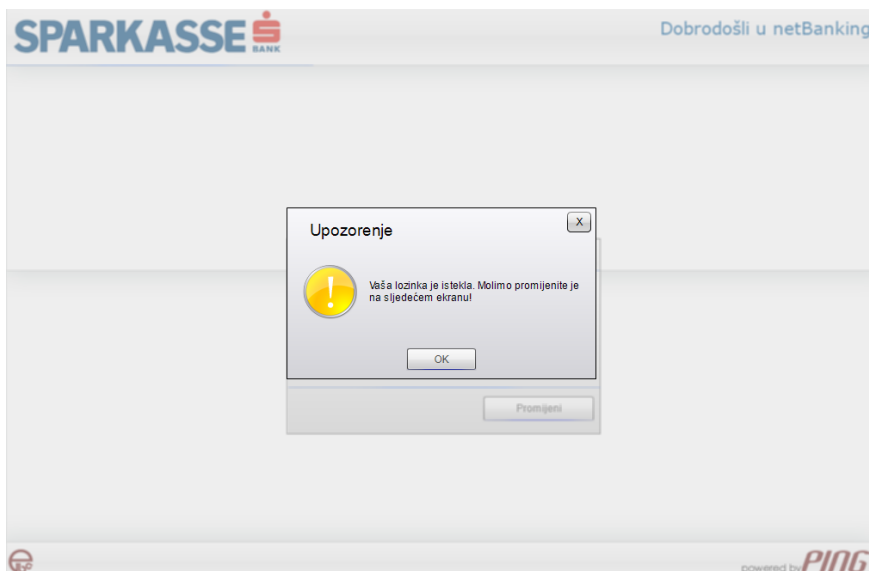
Pokretanjem aplikacije korisnik započinje ulaskom na <http://sparkasse.ba/netbanking/>. Korisnik ima mogućnost izbora jezika aplikacije.

Klikom na opciju „prijava“ otvara se prozor za identifikaciju korisnika gdje je potrebno unijeti korisničko ime i lozinku. Korisničko ime Klijent preuzima od uposlenika banke zajedno sa TOKEN-om, dok lozinku svaki ovlašteni korisnik dobiva putem SMS poruke na broj mobitela koji je unesen na Zahtjevu.



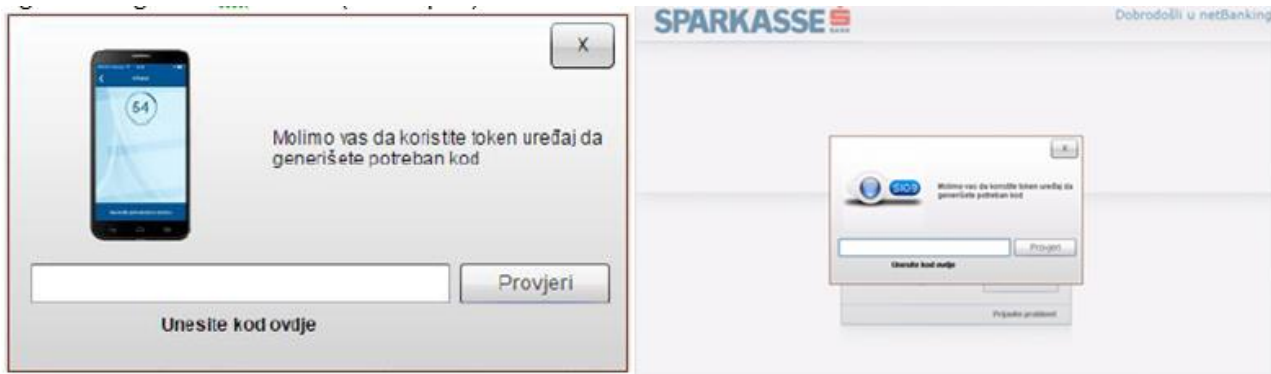
Slika 1 – Početna maska za unošenje korisničkog imena i inicijalne lozinke

Nakon prvog unosa lozinke prosljeđene od strane Banke putem SMS poruke, Klijentu će se odmah pojaviti poruka „vaša lozinka je istekla“ tj poruka za izmjenu/unos nove lozinke (slika ispod).





Slika 2 – poruka za izmjenu inicijalne lozinke

Nakon promjene i unosa nove lozinke, korisnik može kliknuti i checkbox "Zapamti me" tako da „korisničko ime“ ostane zapamćeno, u svrhu lakšeg i bržeg budućeg logiranja. Nakon unosa nove lozinke bitno je da istu zapamtite kako biste prilikom sljedećeg logovanja unijeli ispravnu lozinku. **U slučaju da zaboravite lozinku, dostava nove lozinke na SMS broj Banka naplaćuje u skladu sa Tarifnikom Banke.** Ukoliko korisnik tri puta ukuca pogrešne podatke, aplikacija se zaključava. Otključavanje je moguće pokretanjem aplikacije ponovo nakon 10 minuta nekorištenja aplikacije. Nakon prijave (unosa korisničkog imena i lozinke), otvara se prozor za unos sigurnosnog koda sa tokena (slika ispod).



Slika 3 – Generisanje koda za identifikaciju korisnika (bilo da koristite token ili mToken)

Ukoliko je klijent dobio **veliki KC Token**, nakon uključivanja tokena na zeleno dugme , korisnik kuca osobnu lozinku od 4 broja, i ponovnim klikom na zeleno dugme , token će izbaciti broj koji korisnik kuca u polje „sigurnosni kod“ (slika 4. iznad) i klika „Provjeri“. Ukoliko klijent tek prvi put koristi netbanking, token uključuje i prvi put kuca PIN od četiri nule 0000 i klika na zeleno dugme nakon čega se na ekranu pojavljuje poruka „NOVI PIN“, gdje korisnik treba unijeti novi PIN od četiri broja koju će koristiti svaki sljedeći put pri uključivanju tokena.



KC Token



Mini Token


Ukoliko korisnik tri puta unese pogrešan PIN u token, token se zaključava. U tom slučaju korisnik je obavezan dostaviti TOKEN u poslovnicu gdje je prvi put uzeo postojeći token, gdje će ovlašteni uposlenici banke preuzeti stari i dodijeliti novi token korisniku. Korisnik je obavezan izvršiti plaćanje za uslugu

desinhronizacije tokena u skladu sa cijenama tarifnika Sparkasse banke, a nakon što mu uposlenik banke ispostavi fakturu za izvršenu uslugu.

Ukoliko je klijent od strane uposlenika dobio „**mini token**“, za mini token nema unošenja pin-a, već pritiskom na zeleno dugme displej tokena ispisuje brojeve koje je potrebno unijeti u prozorčić na računaru (slika 3.) kao sigurnosnu provjeru za login.

Ukoliko Klijent koristi mToken potrebno je pogledati posebno uputstvo za korištenje mToken-a dostupno na Internet stranici banke www.sparkasse.ba

2. Korištenje TOKEN-a prilikom potpisivanja/plaćanja naloga

Nakon što korisnik završi sa unošenjem naloga, isti će biti smješteni u tabu “NEPOTPISANI NALOZI” i spremni za potpisivanje tj. za slanje na plaćanje u Banku. **POTPISIVANJE** korisnik vrši tako što ulaskom u tab „nepotpisani nalozi“, bira jedan, ili više naloga (sa opcijom ctrl+klik), ili označava sve naloge (klikom na opciju „označi sve“ na operacionom meniju). Nakon izbora naloga korisnik klika na opciju „**POTPISI**“ koja se nalazi na operacionom meniju iznad naloga. Nakon klika „potpiši“ netbanking izbacuje prazan prozorčić za unos koda i šest brojeva koji se nalaze iznad prozora (ukoliko korisnik koristi veliki – **KC token**). Korisnik uključuje token sa osobnom lozinkom i NE KLIKA zeleno dugme odmah, već odmah nakon unosa osobne lozinke, unosi u token 6 brojeva koji su mu ispisani u prozoru netbanking-a. Nakon unosa brojeva pomoću tokena korisnik tek tada klika na zeleno dugme . Token će na display-u prikazati brojeve koje je potrebno unijeti u prazno polje u prozorčiću u netBankingu i kliknuti „provjeri“. Ukoliko je korisnik ispravno unio brojeve označeni nalozi će biti potpisani i automatski poslani banci na obradu.

Ukoliko Klijent koristi „**mini token**“ prilikom potpisivanja naloga, na aplikaciji na računaru se otvara prozorčić za unos koda. Klikom na zeleno dugme na mini token-u, token izbacuje brojeve koje korisnik unosi u prozorčić na računaru i klika na opciju „provjeri“. Ukoliko je korisnik ispravno unio brojeve sa tokena, označeni nalozi će biti potpisani i automatski poslani banci na obradu.

Prilikom kreiranja i slanja ino naloga, za izvršenje naloga potrebno je da Klijent prilikom kreiranja ino naloga kroz netbanking aplikaciju korištenjem opcije „Prilozi“ (slika ispod) pošalje dokaz kao osnov plaćanja (ugovr, faktura, rezervacija i sl.), ili Banci dostavi dokument koji je osnov plaćanja na faks broj 033 280-240 ili na e-mail adresu swift@sparkasse.ba.

Slika 4: Nalog za ino plaćanje



3. Limiti prilikom vršenja konverzije valuta

Kada su u pitanju konverzije, korisnici – pravna lica mogu vršiti konverzije iz KM u EUR i obratno do limita po jednoj transakciji u iznosu od 100.000,00 protuvrijednosti KM, dok je za sve ostale valute taj limit 25.000,00 protuvrijednosti KM.

Svi iznosi preko limita se prijavljuju nadležnom Sektoru u Sparkasse banci. Naloge preko limita korisnici mogu izvršavati do 16h po kursu koji ponudi Sparkasse banka.

BITNE INFORMACIJE ZA KLIJENTA/KORISNIKA USLUGE

- Za korištenje netBanking aplikacije Klijent je dužan obezbijediti minimalne tehničke uslove: procesor generacije P4 ili jači, minimalno 1 GB memorije, minimalno 200 MB prostora na hard disku, Internet pristup brzine 128 Kbps ili više, grafička kartica sa rezolucijom 1024x768 ili više, operativni sistem WinXPSP2 ili više, Adobe Reader 9.0 ili višu verziju, Internet browser: Chrome verzija 30 ili više (na Win7+, Android 4.1+ ili iOS9+), Firefox verzija 27 pa navise (na WinXPSP2+, Android 4.0.3+ ili iOS 8.2+), Internet Explorer (I IE mobile) verzija 11 (na Win7) pa navise, Android 5.,+ i Windows Phone 8+ za mobilne telefone sa mogućnošću pristupa Internetu. Klijent je obavezan preuzeti najnoviju verziju aplikacije Sparkasse mobilnog bankarstva sa odgovarajućeg marketa („Google Play“, „App Store“ ili Windows Phone Trgovina).
- Klijent se obavezuje čuvati podatke o korisničkom imenu i lozinki, kao i token i aktivacijski ključ, te obavijestiti Banku odmah i bez odlaganja o bilo kom slučaju gubitka ili zloupotrebe korisničkih kredencijala za korištenje aplikacije. Gubitak ili krađu sredstava identifikacije, Klijent (ovlašteni zastupnik, kontakt osoba ili korisnik) je dužan je prijaviti Banci za vrijeme radnog vremena od 08:30 - 17:00 sati, na telefon: 033/280-300 i/ili na e-mail adresu netbanking.pl@sparkasse.ba i/ili nadležnom Voditelju poslovnog odnosa. Gubitak ili krađu mobilnog telefona Klijent je dužan odmah prijaviti Banci lično u bilo kojoj poslovnicu Banke. Klijent snosi svu štetu koja nastane usljed nepridržavanja uputa vezanih za korištenje netBanking i mBanking aplikacije i sredstava identifikacije (tokena) a posebno u slučaju otkrivanja ili činjenja dostupnim lozinki i šifri neovlaštenim trećim licima, činjenja dostupnim sredstava identifikacije (tokena) neovlaštenim trećim licima, neprijavlivanja gubitka, krađe ili neovlaštenog korištenja sredstava identifikacije ili netBanking ili mBanking aplikacije, gubitka ili krađe mobilnog telefona na koji prima SMS poruke ili neprijavlivanja izmjene broja mobilnog telefona na koji prima SMS poruke. Banka će Klijentu blokirati upotrebu netBankinga/mBankinga, ako po prijavi Klijenta ustanovi gubitak, krađu ili neovlašten pristup netBankig/mBanking usluzi ili sredstvima identifikacije. Korištenje usluge/a ponovno će se omogućiti poslije zamjene sredstava identifikacije. Banka ne odgovara Klijentu za štetu koja je nastala njegovim nepridržavanjem uputa vezanih za sigurno korištenje netBanking/mBanking uskuge kao ni za štetu koja je nastala prije prijave neovlaštenog korištenja netBanking/mBanking usluge i blokiranja iste. Nakon obrade Zahtjeva i zaključenja Ugovora, Banka Klijentu uručuje sredstvo za identifikaciju i letak sa kratkim uputama o korištenju. Banka izvršava naloge za plaćanje u skladu s Općim uslovima korištenja te u skladu s ostalim pravovaljanim ugovorima i važećim propisima. Svi postupci korisnika se elektronski bilježe. Elektronski zapis postupaka i naloga se arhiviraju u skladu sa važećim zakonskim propisima. Banka će izvršavati naloge za plaćanje kada su ispunjeni svi uslovi za izvršenje, u skladu sa važećim zakonskim propisima koji regulišu obavljanje platnog prometa. Banka ne odgovara za tajnost informacija nakon njihovog primanja na definisani mobilni telefon Korisnika te nije odgovorna za zloupotrene nastale tim putem. Banka nije dužna provjeravati vlasništvo mobilnog telefona navedenog u Zahtjevu.
- Klijent je dužan koristiti usluge na način propisan uputstvima za korištenje usluga. Uputstva za korištenje usluge su dostupna na Internet stranici Banke www.sparkasse.ba.
- Cut off time (COT) za izvršenje naloga (uslov da je nalog unesen i obrađen u sistemu Banke):
 - Žiro kliring UPP: 15h (unesen i obrađen u sistemu banke)
 - Ino nalozi: 12h (T+0); 14h (T+1 i T+2)
 - RTGS i hitni nalozi: 15:30h
 - UPP nalozi unutar Sparkasse banke: 20:45h

Dodatne napomene:

- Svim novim korisnicima aplikacije, bilo da se prvi put prijavljujete za korištenje aplikacije ili dodajete novog ovlaštenika, lozinka za pristup aplikaciji će biti prosljeđena u vidu SMS poruke na broj mobitela naveden na zahtjevu za konkretnog ovlaštenika, dok korisničko ime i TOKEN uređaj Klijent preuzima od nadležnog uposlenika Banke.
- Ukoliko Korisnik tri puta unese pogrešan PIN u token, token će izbaciti poruku da je zaključan i u tom slučaju potrebno je da Klijent donese token u poslovnicu/filijalu gdje je prvi put uzeo netBanking,

gdje će mu VPO, ili ovlaštena osoba dati novi token. Za navedenu uslugu, Klijentu će biti fakturisana usluga prema tarifniku Sparkasse banke.

- Ukoliko Klijent uspješno unese PIN u token, ali pogriješi u prepisivanju brojeva sa tokena u prozorčić na računaru (koje token izbacila za generisanje u aplikaciju - slika 4.) i ukoliko korisnik pogriješi tri puta, token će biti desinhroniziran i procedura je ista kao i za opisani slučaj iznad.
- Ukoliko korisnik uspješno unese korisničko ime i šifru, ali mu nakon unosa broja sa tokena, javi da je nalog zaključan, token je desinhronizovan te isti treba zamijeniti (na način kako je opisano u prvom slučaju). Ovo se najčešće dešava kada korisnik uključuje token više puta, a ne izvrši logovanje na aplikaciju netBanking-a. Ukoliko Klijent do 10 puta uključi token (od prvog momenta uključivanja), a ne pristupi aplikaciji tj. ne loguje se na netBanking aplikaciju, token će se desinhronizovati i procedura je ista kao i za prva dva slučaja. Ukoliko se korisnik npr. loguje deveti put, brojčanik se resetuje i Klijent ima mogućnost na novih devet pokušaja tj. mogućnost da uključuje token, a da ne pristupi aplikaciji netBanking.
- Ukoliko se desi, da se aplikacija zaključa (sesija istekne, ili korisnik tri puta unese pogrešno korisničko ime, ili lozinku prilikom prijave), aplikacija se otključava nakon 15 minuta nekorištenja od strane korisnika. Nakon 15 minuta, Klijentu će biti ponovo omogućen pristup aplikaciji tj. Klijent se mora ponovo prijaviti kao da nije ni koristio browser. U nekim slučajevima, može se desiti da korisnik mora zatvoriti sve browsere koje ima otvorene, kako bi aplikacija proradila.
- Prilikom promjene lozinke, lozinka mora imati minimalno 8 karaktera sa kombinacijom malih i velikih slova i brojeva. Radi sigurnosti lozinku ćete morati promijeniti svakih 6 mjeseci o čemu ćete dobiti notifikaciju kroz netbanking aplikaciju. Prilikom izmjene lozinke nećete moći ponavljati istu lozinku budući da je sistemski onemogućeno ponavljanje zadnjih 6 lozinki.
- Izmjenu lozinke kada god želite možete raditi neograničen broj puta kroz opciju „Postavke“ u netBanking aplikaciji.
- Zahtjevi koji se odnose na minimalnu opremu koju korisnik mora posjedovati za korištenje Elba aplikacije, uputstva za ispravno postupanje i korištenje aplikacije, postupke koje Klijent mora slijediti u slučaju zloupotrebe, ili sumnji na zloupotrebu, kao opis odgovornosti Klijenta i Banke definisani su Ugovorom koji Klijent potpisuje sa Bankom za korištenje usluge, kao i Općim uslovima poslovanja sa poslovnim subjektima s kojima je Klijent upoznat prilikom potpisivanja Zahtjeva/Ugovora za uslugu.
- Korisničko uputstvo (prošireno i skraćeno) možete preuzeti na web stranici <https://www.sparkasse.ba/bs/pravna-lica/e-bankarstvo/netbanking>

Korisni savjeti:

- Ne zapisujte korisničko ime, lozinku i jednokratnu lozinku sa tokena a pogotovo ih ne ostavljajte na mjesta koja su dostupna drugim ljudima.
- Za lozinku birajte pojmove koje drugi ljudi ne mogu povezati sa Vama.
- Za lozinku (min 8 karaktera) koristite i slova i brojeve.
- Ne povjeravajte lozinku, korisničko ime i jednokratnu lozinku dobijenu sa tokena nikome, čak niti službenicima banke!
- Po prvom pristupu u netBanking/mBanking uslugu, nakon unosa inicijalne lozinke sistemski ćete dobiti poruku za unos nove lozinke.
- Po završetku korištenja usluge, obavezno se odjavite.
- Nipošto ne ostavljajte netBanking aplikaciju bez Vašeg nadzora. Ukoliko napuštate Vaše radno mjesto, zaključajte aplikaciju tako što u glavnom meniju izaberete podmeni *Zaključaj aplikaciju*.
- Na Vaš PC ne instalirajte programe nepoznatih odnosno neprovjerenih autora.
- Na Vaš PC ne instalirajte neprovjerene hardverske uređaje.
- Instalirajte antivirusni program.