Uslovi korišćenja sredstava za autentifikaciju Banca Intesa ad Beograd

Uslovi korišćenja sredstava za autentifikaciju Banca Intesa ad Beograd (u daljem tekstu: Banka), predstavljaju pravila korišćenja i propisuju:

- namenu sredstava za autentifikaciju,
- vrste sredstava za autentifikaciju koja se koriste u sistemu Banke, i
- opšte odredbe korišćenja sredstava za autentifikaciju.

Sredstva za autentifikaciju koja Banka dodeljuje i ustupa na korišćenje Korisniku, namenjena su isključivo za autentifikaciju Korisnika i autorizaciju transakcija u sistemima Banke, pri čemu:

- **autentifikacija korisnika** predstavlja proveru i potvrdu identiteta Korisnika prilikom pristupa sistemima Banke, i
- **autorizacija transakcija** predstavlja potvrdu izvršenja finansijskih i/ili nefinansijskih transakcija u sistemima Banke.

Sredstva za autentifikaciju koja se koriste u Banci su:

1. **mToken** – predstavlja softversko sredstvo za autentifikaciju kompatibilno sa iOS i Android platformama pametnih mobilnih telefona i uređaja, kod kojeg se autentifikacioni parametar generiše u aplikaciji instaliranoj na prenosnom uređaju korisnika. Aplikacija se može preuzeti sa Store-a (Apple Store, Google play store), gde se nalaze i ostale aplikacije za pametne telefone.

2. **SMS OTP** – predstavlja virtuelno sredstvo za autentifikaciju kod kojeg se autentifikacioni parametar generiše na autentifikacionom serveru i dostavlja na uređaj korisnika putem SMS poruke. Slanje parametara se vrši na broj mobilnog telefona koji je Korisnik registrovao u Banci za SMS usluge.

Način korišćenja sredstava za autentifikaciju opisan je u dokumentu „Korisničko uputstvo za sredstva autentifikacije“ koji je dostupan na internet portalu Banke www.bancaintesa.rs.

Sredstva za autentifikaciju se koriste u sledećim sistemima Banke:

1. **Online - aplikacija za internet bankarstvo:**

Korisnik može da koristi mToken i SMS OTP sredstva za autentifikaciju za potrebe:

A. Autorizacije finansijskih i nefinansijskih transakcija u Online aplikaciji

Korisnici koji imaju registrovana oba sredstva za autentifikaciju (mToken i SMS OTP) moći će da koriste na Online aplikaciji isključivo mToken.

2. **Intesa Mobi - aplikacija za mobilno bankarstvo:**

Korisnik može da koristi isključivo mToken sredstvo za autentifikaciju za potrebe:

A. Autentifikacije korisnika, odnosno logovanja u Intesa Mobi aplikaciju
B. Autorizacije finansijskih i nefinansijskih transakcija u Intesa Mobi aplikaciji

Opšte odredbe:

- Banka ima pravo da onemogući korišćenje SMS OTP sredstva za autentifikaciju ukoliko na bilo koji posredan ili neposredan način dođe do saznanja da registrovani broj mobilnog telefona više nije u posedu Korisnika.

- Banka ima pravo da prilikom aktivacije mToken sredstva za autentifikaciju automatski dodeli korisniku i SMS OTP sredstvo za autentifikaciju. Korisnik nema pravo da deaktivira samo SMS OTP sredstvo za autentifikaciju ukoliko ima i aktivno mToken sredstvo za autentifikaciju, već se deaktivacija u ovom slučaju vrši za oba sredstva za autentifikaciju.

- U slučaju da Korisnik ne izvrši logovanje u Intesa Mobi u roku od 7 dana nakon aktiviranja Intesa Mobi usluge na šalteru Banke, usluga mobilnog bankarstva će biti onemogućena. Korisnik naknadno može da zahteva reaktiviranje usluge u Banci.

- U slučaju nekorišćenja dodeljenih sredstava za autentifikaciju, Banka ima pravo da:
  - **privremeno onemogući** upotrebu dodeljenih sredstava za autentifikaciju ukoliko ista nisu korišćena u periodu od **3 meseca** u kontinuitetu. Korisnik naknadno može da zahteva deblokadu dodeljenih sredstava ukoliko želi da nastavi sa njihovim korišćenjem, i
  - **trajno onemogući** upotrebu dodeljenih sredstava za autentifikaciju ukoliko ista nisu korišćena u periodu od **6 meseci** u kontinuitetu. Korisnik naknadno može da zahteva aktivaciju novih sredstava autentifikacije ukoliko želi da ih ponovo koristi.

  Pod nekorišćenjem se podrazumeva da korisnik u posmatranom vremenskom periodu nije izvršio ni jednu autentifikaciju ili autorizaciju preko nijednog od dodeljenih sredstava za autentifikaciju, a bez obzira na rezultat autentifikacije ili autorizacije (uspešna ili ne).

  U slučaju da su se stekli uslovi i da se Banka odlučila za jedno od prethodno navedenih onemogućavanja upotrebe sredstava za autentifikaciju, Banka će o tome obavestiti Korisnika jednim od sledećih načina komunikacije: pisanom ili elektronskom poštom, SMS porukom, objavom na govornom automatu ili telefonskim pozivom od strane zvaničnog Kontakt centra Banke, a u skladu sa registrovanim podacima o Korisniku u Banci.

- Korisnik je u obavezi da preuzete podatke za aktivaciju mToken aplikacije i kreirani PIN za korišćenje mToken aplikacije, čuva na način da oni budu samo njemu dostupni i poznati i da ne mogu doći u kontakt sa neovlašćenim osobama koje bi te informacije mogle da zloupotrebe.

- Preporuka je da PIN koji Korisnik kreira, ne bude lako prepoznatljiv. Treba izbegavati kombinaciju cifara koje odgovaraju Korisnikovom datumu rođenja i sličnim kombinacijama cifara koje ukazuju na Korisnika, ili bliskih osoba sa Korisnikom, koje predstavljaju javno dostupne lične podatke. Preporučljivo je da se odabere što duži niz slučajnih cifara.

- Preporuka je da korisnik na mobilnom uređaju preko kojeg koristi sredstva za autentifikaciju, primenjuje šifrovanje uređaja radi njegovog zaključavanja, na način koji je to aplikativno dozvoljeno na uređaju odnosno. Preporuka je da najmanji nivo bezbednosti podrazumeva unošenje PIN koda ili šifre, poznatih samo korisniku, a radi otključavanja mobilnog uređaja.

- U slučaju postojanja sumnje da je mobilni pretplatnički broj i mobilni uređaj Korisnika preko kojeg se koriste sredstva za autentifikaciju zloupotrebljen, Banka ima pravo da

privremeno ili trajno onemogući korišćenje dodeljenih sredstava za autentifikaciju i da bez odlaganja obavesti Korisnika o potencijalnoj zloupotrebi mobilnog pretplatničkog broja i uređaja.

- Korisnik je dužan da u najkraćem mogućem roku Banci prijavi svaki gubitak, krađu, zloupotrebu, neovlašćeno korišćenje, promenu ili gašenje mobilnog pretplatničkog broja i mobilnog uređaja preko kojeg koristi sredstva za autentifikaciju, i to lično u Banci ili putem zvaničnog Kontakt centra Banke. Banka u tom slučaju ima pravo da privremeno ili trajno onemogući korišćenje dodeljenih sredstava za autentifikaciju. Banka ne snosi odgovornost za finansijsku ili drugu štetu proisteklu kao posledica neprijavljivanja gubitka, krađe, promene ili gašenja mobilnog pretplatničkog broja i mobilnog uređaja, kao i u slučaju zloupotrebe ili neovlašćenog korišćenja Korisnikovog mobilnog pretplatničkog broja, uređaja ili dodeljenih sredstava za autentifikaciju.

- Preporuka Banke je da treba koristi uređaje kojima nije ukinuta sistemska zaštita (rutovanje, džejlbrejkovanje i sl.), odnosno koji koriste antivirus zaštitu i zašitu od krađe. Ne treba vršiti instalaciju aplikacija na mobilnom uređaju koje nisu poreklom od poznatih izdavalaca.

- Sredstva za autentifikaciju su neprenosiva i može ih koristiti samo Korisnik kome su dodeljena. Korisnik ne sme, na bilo koji način, zloupotrebljavati dodeljena sredstva za autentifikaciju.

- Korisnik ima pravo da zahteva prestanak korišćenja sredstava autentifikacije, gde se na inicijativu Korisnika vrši deaktivacija sredstava za autentifikaciju (otkazivanje upotrebe) ili uskraćivanjem prava na korišćenje sredstava za autentifikaciju od strane Banke (zabrana upotrebe).

- Korisnik potvrđuje da je upoznat sa Opštim uslovima poslovanja Banca Intesa ad Beograd u segmentu stanovništva.