POSEBNI USLOVI KORIŠĆENJA USLUGE ELEKTRONSKOG I MOBILNOG BANKARTSVA ZA FIZIČKA LICA, PREDUZETNIKE I POLJOPRIVREDNIKE

I. OPŠTE ODREDBE

1. Prava i obaveze Korisnika sistema elektronskog/mobilnog bankarstva regulišu se ovim Posebnim uslovima korišćenja usluge elektronskog i mobilnog bankarstva za fizička lica, preduzetnike i poljoprivrednike (**u daljem tekstu: Posebni uslovi**), Terminskim planom poslovanja po platnim računima fizičkih lica, preduzetnika i poljoprivrednika, Tarifom za opšte bankarske usluge fizičkim licima i poljoprivrednicima, Tarifom za opšte bankarske usluge preduzetnicima (u daljem tekstu: **Tarife za opšte bankarske usluge**), a koji su sastavni deo Okvirnog ugovora Korisnika.
2. Upotreba sistema elektronskog/mobilnog bankarstva predstavlja uslugu koju Banka pruža isključivo Klijentima Banke, odnosno fizičkim licima/preduzetnicima/poljoprivrednicima koji imaju otvoren račun, koji uključuje usluge elektronskog/mobilnog bankarstva.
3. Informacija o ponudi proizvoda elektronskih kanala i uslugama koje Korisnik može obavljati korišćenjem određenih proizvoda elektronskog/mobilnog bankarstva dostupna je u poslovnoj mreži Banke i na internet stranicama Banke www.unicreditbank.rs.
4. Za svaki ugovoreni proizvod elektronskog/mobilnog bankarstva Banka će omogućiti Korisniku uvid u sve neophodne informacije u vezi sa korišćenjem izabranog proizvoda kao i korišćenje svih usluga navedenih u Zahtevu kao i u ovim Posebnim uslovima.
5. Podnošenjem Zahteva, Klijent potvrđuje da je upoznat i saglasan sa svim odredbama ovih Posebnih uslova i da ih u potpunosti prihvata.
6. Korisnik je odgovoran za tačnost svih podataka neophodnih za ispravno i sigurno funkcionisanje ugovorenog proizvoda elektronskog/mobilnog bankarstva koje je predao Banci, i dužan je da obavesti Banku o svakoj njihovoj promeni (npr. broj telefona, broj i model mobilnog telefona, e-mail adresa i drugo).
7. Za korišćenje pojedinih proizvoda elektronskog bankarstva Korisnik mora osigurati odgovarajuću računarsku infrastrukturu. Tehnički zahtevi za korišćenje pojedinih proizvoda objavljeni su na internet stranicama Banke www.unicreditbank.rs i/ ili su dostupni u poslovnoj mreži Banke. Korisnik je, u zavisnosti od tehničkih zahteva pojedinačnog proizvoda elektronskog bankarstva, dužan da Banku obavesti o vrsti opreme koju koristi kako bi proizvod funkcionisao na ispravan način.
8. Ovi uslovi poslovanja uređuju uslove i načine korišćenja elektronskih platnih instrumenata Banke, te prava, obaveze i odgovornosti koje u pogledu njihovog ugovaranja i korišćenja imaju fizička lica, preduzetnici i poljoprivrednici (**u daljem tekstu: Korisnici**), kao i fizička lica ovlašćena za korišćenje elektronskih platnih instrumenata u ime preduzetnika (**u daljem tekstu: Krajnji korisnici**) i Banka.
9. Podaci koje Banka prosleđuje Korisniku ili Krajnjem korisniku proizvoda elektronskog i mobilnog bankarstva imaju istu vrednost kao i dokumenti koje Banka šalje poštom i mogu ih zameniti.

II. ZNAČENJE POJEDINIH POJMOVA

Pojedini pojmovi korišćeni u ovim Posebnim uslovima imaju sledeće značenje:

1. **Korisnik** je fizičko lice, preduzetnik ili poljoprivrednik koji s Bankom ugovori korišćenje nekog od proizvoda elektronskog/mobilnog bankarstva;
2. **Krajnji korisnik (ovlašćenik)** je fizičko lice koje je Korisnik ovlastio za korišćenje određenog proizvoda elektronskog bankarstva u ime i za račun Korisnika;
3. **Korisničko ime** je jedinstveni niz alfanumeričkih znakova, koji predstavlja jedan od elemenata kojima se Krajnji korisnik identifikuje pri procesu registracije za uslugu elektronskog bankarstva;
4. **Potpisnik** je Korisnik/Krajnji korisnik koji poseduje uređaj na kome je smeštena elektronska autorizacija, i koji je Zahtevom ovlašćen da u ime Korisnika potpisuje (autorizuje) platne naloge i druge instrukcije i poruke Banci
5. **Korisničko uputstvo** je pisani dokument, koji opisuje način registracije Korisnika i/ili Krajnjeg korisnika i korišćenja proizvoda elektronskog/mobilnog bankarstva.
6. **Šifra Za Otključavanje/Lozinka** je kod/lozinka koja se koristi za otključavanje pametne kartice ili USB Ključa, u slučaju kada se pametna kartica ili USB Ključ zaključaju usled uzastopnog unosa pogrešnog PIN-a. U slučaju zaključavanja tokena neophodno je ispratiti procedure dostavljanja LOCK PIN-a zaključanog tokena Banci od strane klijenta, i dostavljanja neophodnih podataka za otključavanje klijentu od strane Banke, kako bi token bio otključan.
7. **Enkripcija** je postupak kojim se neki podatak pretvara u oblik koji je čitljiv samo primaocu kojem je namenjen.
8. **Dekripcija** je postupak kojim primalac enkriptovani podatak čini čitljivim.

9. **Elektronski kanali** su sredstva i oblici elektronske komunikacije koji omogućavaju korišćenje i/ili ugovaranje pojedinih bankarskih i nebankarskih usluga bez istovremenog fizičkog prisustva Korisnika/Krajnjeg korisnika i službenika Banke na istom mestu, a obuvataju mrežu usluga koje Banka stavlja na raspolaganje Korisniku: elektronsko bankarstvo (Online banking, mBanking, BusinessNet Professional, Multicash, Halcom), kao i povezivanje korišćenjem drugih kanala elektronskog povezivanja koje Banka omogući Korisniku;
10. **Pametna kartica i USB Ključ** su Sertifikovani kriptografski uređaji koji služe za siguran smeštaj elektronskih sertifikata;
11. **Sertifikat** je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju korisnika usluga;
12. **Elektronski potpis** je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
13. **Kvalifikovani elektronski potpis** je elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, a koji ispunjava uslove utvrđene Zakonom o elektronskom potpisu;
14. **Aktivacioni kod** je niz slova i brojeva koji Banka dostavlja klijentu u svrhu aktivacije mobilne aplikacije za elektronsko bankarstvo ili mobilnog tokena. Ovaj kod je jedinstven i jednokratan, a njegova važnost je vremenski ograničena.
15. **QR kode** (eng. QR – Quick Response) je standardizovana dvodimenzionalna oznaka koja predstavlja dvodimenzionalni barkod zasnovan na ISO 18004.

III. VRSTE I OPSEG USLUGA I SISTEM SIGURNOSTI

1. Banka Korisnicima pruža sledeće vrste usluga elektronskog bankarstva:
- Global Web Solution (u daljem tekstu GWS)- sistem za elektronsko bankarstvo (**Online banking -** za fizička lica, **BusinessNet Professional** - za preduzetnike),
- HAL e-bank sistem za elektronsko bankarstvo (u daljem tekstu: **HAL e-bank**) za preduzetnike
- MultiCash sistem za elektronsko bankarstvo (u daljem tekstu: **MultiCash**) za preduzetnike
- Mobile Banking - sistem za elektronsko bankarstvo preko mobilnog telefona (u daljem tekstu: **mBanking**) za fizička lica
- Mobile Banking - sistem za elektronsko bankarstvo preko mobilnog telefona (u daljem tekstu: **mBusiness**) za pravna lica
- SWIFTNET MT101 za preduzetnike
- E- izvod servis za preduzetnike.

2. **Online banking** predstavlja način komunikacije Korisnika sa Bankom elektronski, odnosno putem Internet pretraživača kojim pristupa sajtu Banke, a koja Korisniku omogućava brzu i efikasnu realizaciju bankarskih usluga bez obaveze Korisnika da poseti ekspozituru Banke. Ova aplikacija koristi mehanizam tokena i vremenskih lozinki za pristup sistemu i potpisivanje naloga. Da bi se Klijentima obezbedio visok nivo sigurnosti podataka koriste se tri nivoa zaštite: lična identifikacija, identifikacija putem tokena (privremenu lozinku) i SSL/TLS enkripcija.

2.1. **Token** je elektronski uređaj koji se dobija pri uspostavljanju korišćenja Online banking rešenja za elektronsko bankarstvo. Korisnik u token unosi PIN kod, nakog čega token generiše vremensku lozinku koja važi 30 sekundi, a koristi se za prijavu na Online banking aplikaciju. Korisnik sam određuje PIN kod koji će koristiti i može ga promeniti u bilo kom trenutku. Alogoritmi funkcionisanja token uređaja su službena tajna.

2.2. **Mobilni token (u daljem tekstu: mToken)** - u okviru mBanking/mBusiness aplikacije, koja se instalira na mobilnom telefonu, postoji mogućnost korišćenja softverskog tokena, programa koji, nakon unosa PIN koda, generiše jednokratne lozinke koje Korisnik/Krajnji korisnik koristi za autentifikaciju i potpisivanje platnih naloga u Online banking aplikaciji. Prilikom aktivacije mTokena, od Korisnika će se tražiti da unese korisničko ime, kao i aktivacioni kod, nakon čega će Korisniku biti omogućeno da kreira svoj lični PIN kod. Na ovaj način, aplikacija omogućava da klijent koristi mobilni telefon ili tablet kao token.

2.3. **SSL/TLS PROTOKOL** je Enkripcija sa 256-bitnim ključem je industrijski standard u bezbednim internet komunikacijama. Koristi ga 99% važnih internet prezentacija kao što su banke, kompanije za online ulaganja, berzanske transakcije ili kupovinu.

2.4. **Korisničko ime** je jedinstveni niz alfanumeričkih znakova koji predstavlja jedan od elemenata kojima se Korisnik identifikuje pri procesu registracije. Klijent se predstavlja putem lične identifikacije (username) i dokazuje svoj identitet pomoću privremene lozinke koju generiše token, nakon čega se dozvoljava pristup sistemu.

Korisniku su dostupne sledeće usluge putem Online banking aplikacije:
- pristup računu preko sajta Banke uz korišćenje korisničkog imena i lozinke koja se generiše uz pomoć tokena
- realizovanje platnih transakcija u domaćem platnom prometu i platnom prometu sa inostranstvom uz obezbeđivanje neophodne dokumentacije predviđene propisima,
- prenos sredstava u okviru sopstvenih računa Korisnika
- kreiranje naloga za plaćanje sa datumom izvršenja u budućnosti,

- ispostavljanje trajnih naloga za plaćanje u domaćem platnom prometu,
- uvid u stanje i transakcije po svim računima (uključujući i kredite),
- upit u stanje po računu u realnom vremenu,
- pregled stanja na platnim i kreditnim karticama (podaci, transakcije),
- konverzija stranih valuta u dinare po kupovnom kursu Banke, u okviru sopstvenih računa
- konverzija dinara u strane valute po prodajnom kursu Banke, u okviru sopstvenih računa
- razmenu poruka elektronskim putem između Korisnika i Banke,
- udaljeno ispostavljanje naloga Banci (kao npr. promena limita za ispostavljanje naloga, dodavanje računa i sl.),
- dostupnost pregledu kursnih lista,
- dostava obaveštenja od strane Banke ukoliko se Korisnik opredeli za ovaj kanal komunikacije
- primanje korisnih informacija (kontakti u slučaju potrebe, informacije o aktuelnim ponudama koje su prilagođene Korisniku, razna obaveštenja).

3. **BusinessNet Professional** je aplikacija elektronskog bankarstva putem internet konekcije, proizvod UniCredit Banke. Ova aplikacija koristi mehanizam tokena i vremenskih lozinki za pristup sistemu i potpisivanje naloga. Da bi se Klijentima obezbedio visok nivo sigurnosti podataka, BusinessNet Professional koristi tri nivoa zaštite: ličnu identifikaciju, identifikaciju putem tokena (privremenu lozinku) i SSL/TLS enkripciju.

3.1. **Token** je elektronski uređaj koji se dobija pri uspostavljanju korišćenja rešenja za elektronsko bankarstvo BusinessNet Professional. Korisnik u token unosi PIN kod, nakog čega token generiše vremensku lozinku koja važi 30 sekundi, a koristi se za prijavu na BusinessNet Professional aplikaciju. Korisnik sam određuje PIN kod koji će koristiti i može ga promeniti u bilo kom trenutku. Alogoritmi funkcionisanja token uređaja su službena tajna.

3.2. **Mobilni token (u daljem tekstu: mToken)**- u okviru aplikacije mBusiness, koja se instalira na mobilnom telefonu, postoji mogućnost korišćenja softverskog tokena, programa koji, nakon unosa PIN koda, generiše jednokratne lozinke koje Korisnik/Krajnji korisnik koristi za autentifikaciju i potpisivanje platnih naloga u BusinessNet Proffesional sistemu za elektronsko bankarstvo. Prilikom aktivacije mTokena, od Korisnika će se tražiti korisničko ime kao i aktivacioni kod, nakon čega će Korisniku/Krajnjem korisniku biti omogućeno da kreira svoj lični PIN kod. Na ovaj način, aplikacija omogućava da klijent koristi mobilni telefon kao token. Alogoritam generisanja sa Bančinim serverom su službena tajna.

3.3. **SSL/TLS PROTOKOL** je Enkripcija sa 256-bitnim ključem je industrijski standard u bezbednim internet komunikacijama. Koristi ga 99% važnih internet prezentacija kao što su banke, kompanije za online ulaganja, berzanske transakcije ili kupovinu.

3.4. **Korisničko ime** je jedinstveni niz alfanumeričkih znakova koji predstavlja jedan od elemenata kojima se Krajnji korisnik identifikuje pri procesu registracije za uslugu **BusinessNet Professional**. Klijent se predstavlja putem lične identifikacije (username) i dokazuje svoj identitet pomoću privremene lozinke koju generiše token, nakon čega se dozvoljava pristup sistemu.

U domenu platnih usluga, Korisnik može davati dva tipa ovlašćenja u okviru BusinessNet Professional svojim Krajnjim korisnicima na računima i to:

i. Sva prava što podrazumeva sledeća ovlašćenja:
   a. administraciju
   b. unos naloga
   c. potpisivanje naloga - potpis i potpisnički dnevni i transakcioni limiti su direktno određeni kroz Zahtev Klijenta, a u skladu sa tehničkim mogućnostima sistema
   d. konverzija ino valute u domaću valutu
   e. pregled izveštaja pristiglih od Banke
   f. slanje potpisanih naloga u Banku.

ii. Bez prava potpisa, što podrazumeva sva napred navedena prava Korisnika/Krajnjeg korisnika osim pravo na potpis.

Ugovoreni opseg usluga po navedenom servisu se može naknadno promeniti uz korišćenje već postojećih sigurnosnih sredstava.

4. **HAL e-Bank** je softverski proizvod Halcom Informatike d.d. Ljubljana, pod nazivom HAL e-bank. Kod HAL e-bank, u cilju obezbeđivanja sigurnog elektronskog poslovanja sa Bankom uvedena su dva tipa sigurnosnih sredstava i to:

4.1. **HALCOM sertifikat na pametnoj kartici ili USB ključu** je elektronski, identifikacioni instrument koji omogućava Korisniku/Krajnjem korisniku da radi na tekućim računima Korisnika otvorenim kod Banke. Prava Krajnjeg korisnika na tekućim računima Korisnika su tačno definisana na Zahtevu za elektronsko bankarstvo. Korišćenjem digitalnog sertifikata onemogućuje se lažno predstavljanje, odnosno obezbeđuje se pouzdana autentifikacija Korisnika/Krajnjeg korisnika.

Kvalifikovani elektronski sertifikat je elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata (u ovom slučaju HALCOM) koji sadrži podatke predviđene zakonom. Kvalifikovani elektronski sertifikati potvrđuju vezu između javnog kriptografskog ključa Korisnika i identiteta Krajnjeg korisnika koji je izvršio potpisivanje elektronskog dokumenta. Kvalifikovani elektronski sertifikati i pripadajući privatni kriptografski ključevi koriste se za kvalifikovano elektronsko potpisivanje datoteka ili poruka i autentikaciju Korisnika. Kvalifikovani elektronski potpis je elektronski potpis koji ispunjava uslove utvrđene zakonom i kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj.
Korisnik prihvata digitalni sertifikat kao isključivu potvrdu o njegovom identitetu prilikom korišćenja usluga HAL e-bank sistema elektronskog bankarstva, bez prava naknadnog poricanja.
Pametne kartice se izdaju sa utvrđenim rokom važnosti digitalnog sertifikata, a nakon isteka tog roka, važnost digitalnog sertifikat se mora obnoviti. Prilikom izdavanja nove kartice, Korisnik ovlašćuje Krajnjeg korisnika za rad na svojim računima, slanjem novog Zahteva.
U slučaju povlačenja - otkaza prava korišćenja pametne kartice za pojedine Krajnje korisnike, potrebno je pismeno dostaviti Banci Zahtev za otkaz sertifikata i korišćenje usluga HAL e-bank za konkretnog Krajnjeg korisnika.

4.2. **WEB korisničko ime** omogućava Korisniku pravo pristupa WEB HAL e-bank sistemu (**u daljem tekstu: WEB e-banking**). Ovaj sistem predstavlja nadogradnju HAL e-bank i služi za pristup korisnika aplikaciji putem internet pretraživača.
Krajnji korisnici WEB e-b@nking-a sa ovlašćenjem za potpisivanje naloga mogu da udaljeno potpišu naloge uz korišćenje internet pretraživača, WEB korisničkog imena i pripadajuće lozinke, pametne kartice i čitača pametne kartice.
Krajnji korisnici sa pravom pristupa WEB e-b@nking koji imaju ovlašćenje za pregled izveštaja mogu da prate promet i stanje na računima Korisnika korišćenjem samo internet pretraživača, korisničkog imena i lozinke.
Pomoću WEB korisničkog imena Krajnjem korisniku je omogućen pristup računima u skladu sa ovlašćenjima navedenim u inicijalnom Zahtevu Korisnika, a putem WEB HAL e-bank aplikacije.
U slučaju povlačenja - otkaza prava korišćenja WEB korisničkog imena za Krajnjeg korisnika potrebno je da Korisnik dostavi Banci potpisani Zahtev za povlačenje - otkaz prava na korišćenje WEB korisničkog imena.
U slučaju povlačenja - otkaza prava korišćenja pametne kartice za Krajnjeg korisnika, automatski se ukida i pravo na korišćenje WEB korisničkog imena ako je izdato navedenom licu. Zahtev za povlačenje - otkaz prava na korišćenje je potrebno dostaviti Banci u pisanoj formi.

U domenu platnih usluga, Korisnik može davati dva tipa ovlašćenja u okviru Hal e-Bank svojim Krajnjim korisnicima na računima i to:

i. Sva prava, što podrazumeva sledeća ovlašćenja:
   a. administraciju
   b. unos naloga
   c. potpisivanje naloga - potpis i potpisnički dnevni i transakcioni limiti su direktno određeni kroz Zahtev Klijenta, a u skladu sa tehničkim mogućnostima sistema
   d. priprema naloga bez prava pregleda
   e. pregled izveštaja pristiglih od Banke
   f. slanje potpisanih naloga u Banku.

ii. Bez prava potpisa, što podrazumeva sva napred navedena prava Korisnika/Krajnjeg korisnika osim pravo na potpis.

Ugovoreni opseg usluga po navedenom servisu se može naknadno promeniti uz korišćenje već postojećih sigurnosnih sredstava.

5. **MultiCash sistem** za elektronsko banakrstvo je softver za elektronsko bankarstvo proizvođača Omikron Systemhouse iz Kelna, Nemačka. Sistem sigurnosti kod ovog sistema podrazumeva:

5.1. **BPD datoteka** je sigurnosni mehanizam u obliku datoteke uskladištene na određenom nosaču podataka koja u kombinaciji sa elektronskim potpisom omogućava Krajnjem korisniku da radi na tekućim računima Korisnika otvorenim kod Banke. Prava Krajnjeg korisnika na tekućim računima Korisnika su tačno određena na Zahtevu. Korišćenjem BPD datoteke i elektronskog potpisa onemogućuje se lažno predstavljanje, odnosno obezbeđuje se pouzdana autentifikacija Krajnjeg korisnika.

5.2. **Elektronski potpis (ES par ključeva)** je sigurnosni mehanizam u obliku datoteke uskladišten na odgovarajućem nosaču podataka. Kreiranje elektronskog potpisa tj. ES para ključeva obavlja Korisnik u svojoj MultiCash aplikaciji. Uz pomoć BPD datoteke i šifre za komunikaciju, a nakon kreiranja para ključeva za elektronski potpis (ES par ključeva), Korisnik je dužan da napravi inicijalno povezivanje sa Bančinim serverom i da pošalje podatke o svom javnom ključu ES para ključeva koji je generisao.
Privatni ključ ES para ključeva elektronskog potpisa je obezbeđen tajnom lozinkom koju unosi Krajnji korisnik u procesu generisanja ES para ključeva. Lozinka za ES par ključeva

je poznata samo Krajnjem korisniku koji je vlasnik ES para ključeva za potpisivanje. Prilikom inicijalnog povezivanja MultiCash aplikacija štampa dokument sa ispisom javnog ključa Korisnika (Inicijalizaciono pismo korisnika) koje je potrebno da bude potpisano od strane Krajnjeg korisnika i dostavljeno Banci, a kako bi elektronski potpis Krajnjeg korisnika bio odobren za upotrebu na MultiCash sistemu.
Korisnik prihvata BPD datoteku i ES par ključeva (elektronski potpis) kao isključivu potvrdu o njegovom identitetu prilikom korišćenja usluga MultiCash sistema elektronskog bankarstva, bez prava naknadnog poricanja. Po odobrenju Zahteva, Banka uručuje BPD datoteku Krajnjem korisniku tj. licu koje je ovlašćeno za to od strane Korisnika.
Ukoliko Korisnik želi da povuče (otkaže) pravo korišćenja MultiCash sistema za konkretnog Krajnjeg korisnika, potrebno je da pismeno dostavi Banci Zahtev za otkaz korišćenja usluga za MultiCash sistem elektronskog bankarstva za to lice, nakon čega će mu Banka ukinuti prava na MultiCash sistemu.

U domenu platnih usluga, Korisnik može davati dva tipa ovlašćenja u okviru MultiCash svojim Krajnjim korisnicima na računima i to:

i. Sva prava, što podrazumeva sledeća ovlašćenja:
   a. pravo na komunikaciju sa Bankom koja podrazumeva slanje već potpisanih naloga i preuzimanje izveštaja od Banke;
   b. pravo na potpisivanje naloga - kategorija potpisa i potpisnički dnevni i transakcioni limiti su direktno određeni kroz Zahtev Klijenta, a u skladu sa tehničkim mogućnostima sistema.
ii. Bez prava potpisa uključuje pravo na komunikaciju sa Bankom, formiranje naloga za plaćanje, ali bez prava potpisa.

MultiCash sistem, tehnički omogućava na strani dostupnoj Korisniku, definisanje i dodelu prava drugim Krajnjim korisnicima, koji nisu utvrđeni Zahtevom za aktivaciju ovog servisa. Administracija lokalnih Korisnika detaljno je objašnjena u Uputstvu za upotrebu programa. Odgovornost za pravilnu administraciju ovih Krajnjih korisnika je u potpunosti na strani Korisnika. Banka ne snosi nikakvu odgovornost u slučaju pogrešnog podešavanja ovih lokalnih naloga Krajnjih korisnika kao i za sve eventualne zloupotrebe prava koja su lokalno dodeljena.

Ugovoreni opseg usluga po navedenom servisu se može naknadno promeniti uz korišćenje već postojećih sigurnosnih sredstava.

6. **mBanking** predstavlja komunikaciju Korisnika sa Bankom elektronski, putem aplikacije koja se instalira na mobilnom telefonu ili tabletu, a koja Korisniku omogućava brzu i efikasnu realizaciju bankarskih usluga, bez obaveze Korisnika da poseti ekspozituru Banke. Kod UniCredit mBanking aplikacije predviđene su mere radi obezbeđivanja sigurnog elektronskog poslovanja sa Bankom, kao što je kreiranje PIN koda od strane samog Korisnika (koji je na taj način poznat samo njemu), neophodnost upisivanja korisničkog imena i aktivacionog koda, prilikom aktiviranja aplikacije i kreiranja svog PIN koda. Aplikacija je zaštićena od kopiranja i instaliranja na druge telefone, jer se link i aktivacioni kod za instaliranje aplikacije mogu iskoristiti samo jednom (jednokratno). Nije moguće instalirati istu aplikaciju koja je vezana za isti račun na dva različita mobilna uređaja. Preuzimanjem aplikacije za mBanking, instalira se softverski token koji garantuje potpunu sigurnost rada. Aktivacioni kod predstavlja poseban identifikacijski broj koji služi za aktivaciju usluge i nakon toga nije upotrebljiv za dalje korišćenje.

   Korisniku su dostupne sledeće usluge putem mBanking aplikacije:
   - plaćanje svih vrsta računa u domaćem platnom prometu
   - prenos sredstava u okviru sopstvenih računa Korisnika
   - plaćanje na prodajnom mestu
   - dostupnost pregleda kursne liste
   - uvid u stanje i transakcije po svim računima (uključujući i kredite)
   - pregled stanja na platnim i kreditnim karticama (podaci, transakcije)
   - konverzija valuta ,
   - mKeš, podizanje gotovine na bankomatima UniCredit Banke
   - primanje korisnih informacija (informacije o aktuelnim ponudama, razna obaveštenja)
   - podešavanje aplikacije (promena PIN koda, jezika, i sl.)
   - kao i eventualne dodatne usluge koje će Banka razviti u okviru mBanking aplikacije, a o kojima će klijenti biti obavešteni putem ugovorenih kanala komunikacije.

7. **mBusiness** predstavlja komunikaciju Korisnika sa Bankom elektronski, putem aplikacije koja se instalira na mobilnom telefonu, a koja Korisniku/Krajnjem korisniku omogućava brzu i efikasnu realizaciju bankarskih usluga, bez obaveze Korisnika da poseti ekspozituru Banke. Kod UniCredit MBusiness aplikacije predviđene su mere radi obezbeđivanja sigurnog elektronskog poslovanja sa Bankom, kao što je kreiranje PIN koda od strane samog Korisnika (koji je na taj način poznat samo njemu), neophodnost upisivanja lične identifikacije i

aktivacionog koda, prilikom aktiviranja aplikacije i kreiranja svog PIN koda. Aplikacija je zaštićena od kopiranja i instaliranja na druge telefone, jer se link i aktivacioni kod za instaliranje aplikacije mogu iskoristiti samo jednom (jednokratno). Nije moguće instalirati istu aplikaciju koja je vezana za isto korisničko imena dva različita mobilna uređaja. Preuzimanjem aplikacije MBusiness, instalira se softverski token koji garantuje potpunu sigurnost rada. Aktivacioni kod predstavlja poseban identifikacijski broj koji služi za aktivaciju mBusiness usluge i nakon toga nije upotrebljiv za dalje korišćenje.

Korisniku su dostupne sledeće usluge putem MBusiness aplikacije:

- izvršenje platnih naloga u domaćem platnom prometu
- prenos sredstava u okviru sopstvenih računa Korisnika
- plaćanje na prodajnom mestu
- pregled kursne liste
- uvid u stanje i transakcije po svim računima
- pregled stanja i prometa na platnim karticama
- primanje korisnih informacija (informacije o aktuelnim ponudama, razna obaveštenja)
- podešavanje aplikacije (promena PIN koda, jezika, i sl.)
- kao i eventualne dodatne usluge koje će Banka razviti u okviru mBiznis aplikacije, a o kojima će klijenti biti obavešteni putem ugovorenih kanala komunikacije.

8. **SWIFTNET MT101** je usluga kojom se omogućujue da klijenti centralizuju svoj platni Promet. Ove poruke se primaju putem SWIFT poruka. Naloge klijenta koji se šalju putem ovih poruka, a na osnovu Ugovora između Banke I Klijenta, Banka prima i izvršava sa računa Klijenta u domaćoj ili inostranoj valuti a u skladu sa dobijenim instrukcijama.

9. **E-izvod** je servis UniCredit Banke koji omogućava dostavu izvoda po računu, kao i drugih vidova obaveštenja u vezi sa poslovnim odnosom Korisnika i Banke, elektronskim putem na e-mejl adresu.

IV. UGOVARANJE KORIŠĆENJA, OBAVEZE I ODGOVORNOSTI UGOVORNIH STRANA

Uslov za aktivaciju usluga elektronskog bankarstva je da Korisnik otvori tekući račun u Banci, a kako bi mogao da koristi neki od proizvoda elektronskih platnih instrumenata. Korisnik može istovremeno koristiti jedan ili više proizvoda elektronskog bankarstva. Za ugovaranje pojedinačnih proizvoda elektronskog bankarstva Korisnik je u obavezi da Banci dostavi ispravno popunjen i potpisan Zahtev predviđen za ugovaranje tog direktnog kanala. Overom Zahteva za ugovaranje proizvoda elektronskog bankarstva Korisnik potvrđuje da je upoznat sa ovim Posebnim uslovima, Tarifama za opšte bankarske usluge, kao i Opštim uslovima pružanja platnih usluga fizičkim licima, preduzetnicima i poljoprivrednicima, da ih u potpunosti prihvata i da se istim uređuje ugovorni odnos. Korisnik ovlašćuje Banku da direktno zaduži njegov tekući račun za troškove održavanja sistema i sigurnosne opreme, a koje naknade su navedene u Tarifama za opšte bankarske usluge.

Banka ima pravo provere podataka i prikupljanja dodatnih informacija o podnosiocu Zahteva. Podaci koji se odnose na Korisnika, navedeni u Zahtevu za ugovaranje proizvoda elektronskog bankarstva, koji je Banka poslednji primila, smatraće se tačnim i primenjuju se na sve ostale proizvode elektronskog bankarstva koje Korisnik već koristi.

Korisnik je u obavezi da odredi jednog ili više Krajnjih korisnika, koji će u njegovo ime koristiti ugovoreni proizvod elektronskog bankarstva. Za određenog Krajnjeg korisnika moguće je odabrati različite vrste ovlašćenja. Odabir, promena i opoziv ovlašćenja Krajnjih korisnika se temelje na dostavljanju ispravno popunjenih Zahteva Banke predviđenih za pojedinačni ili više proizvoda elektronskog bankarstva, koje Korisnik dostavi Banci na način predviđen za pojedinačni proizvod elektronskog bankarstva.

Banka ima pravo provere podataka i prikupljanja dodatnih informacija o podnosiocu Zahteva. Banka ima pravo da ne ostvari poslovnu saradnju sa Korisnikom. U slučaju odbijanja Zahteva, Banka nije dužna da obrazloži svoju odluku.

Ukoliko Korisnik ne ispunjava obaveze sadržane u ovim Posebnim uslovima, a koje je prihvatio potpisivanjem Zahteva, Banka zadržava pravo da dostavom Obaveštenja jednostrano prekine pružanje usluga sistema elektronskog bankarstva.

Korisnik može otkazati dalje korišćenje sistema elektronskog bankarstva isključivo pisanim putem.

Sva zaduženja nastala pre dana otkaza upotrebe sistema elektronskog bankarstva, periodične troškove koji se odnose na period u kome je otkaz izvršen, kao i sve eventualne troškove i kamate koji proističu iz zaduženja, snosi Korisnik.

1. GWS - BusinessNet Professional, Online banka, mBanking i mBusiness

Ugovaranje korišćenja

1.1 Korisnik dobija mogućnost korišćenja BusinessNet Professional/mBusiness podnošenjem Zahteva od strane ovlašćenog potpisnika, u kome se opredeljuje za ovu vrstu servisa. Ovim Zahtevom, Korisnik ovlašćuje određena fizička lica za rad u GWS-u, određuje pristup računima, i navodi vrstu ovlašćenja tih lica po računima. Korisnik u potpunosti prihvata odgovornost za tačnost unetih podataka.
1.2 Korisnik dobija mogućnost korišćenja Online banking/mBanking aplikacije, podnošenjem popunjenog i potpisanog Zahteva.
1.3 Banka upoznaje Korisnika sa načinom na koji pristupa Online banking/mBanking/mBusiness aplikaciji putem Lične identifikacije i PIN koda. Ličnu identifikaciju bira Korisnik i unosi u Zahtev .

Odgovornosti ugovornih strana

Korisnik preuzima obavezu da će se u radu sa GWS/mBanking/mBusiness sistemom elektronskog bankarstva, u potpunosti pridržavati važećih zakonskih propisa i uputstava za upotrebu za ovaj softverski proizvod.
Korisnik je dužan da čuva, i preuzima obavezu da od Krajnjeg korisnika zahteva da čuva, token kao i tajnost PIN koda, kako oni ne bi došli u posed trećih lica. Ukoliko Korisnik/Krajnji korisnik sumnja ili ustanovi da je neko saznao njegov PIN kod potrebno je da promeni PIN, na način opisan u Korisničkom uputstvu.
Korisnik mBanking/mBusiness aplikacije izjavljuje da je upoznat sa činjenicom da je dužan da čuva PIN kod, i da se aplikacija blokira nakon tri neuspešna unosa PIN koda, kao i da Banka ne snosi nikakvu odgovornost za taj slučaj. U cilju zaštite, Korisnik mBanking/mBusiness aplikacije je dužan da u određenim vremenskim intervalima vrši promenu svog PIN koda, a obavezno ukoliko sumnja ili ustanovi da je neko saznao njegov PIN kod. Korisnik može u bilo kojem trenutku da promeni PIN kod, na način opisan u Korisničkom uputstvu.
Korisnik snosi svu štetu nastalu zbog gubitka, neovlašćenog ili neodgovarajućeg korišćenja tokena ili aplikacije za mBanking/mBusiness.
Korisnik je odgovoran za tačnosti svih podataka dostavljenih Banci i obavezan je da prijavi svaku promenu tih podataka. Ukoliko Banka sama dođe do saznanja da su podaci o Korisniku/Krajnjem korisniku netačni ili izmenjeni, može uskratiti dalje korišćenje usluga GWS, uz naknadno obaveštenje Korisniku.
Korisnik je obavezan da na računarima sa kojih će koristiti usluge UniCredit e-banking-a obezbedi licenciran, pravilno konfigurisan operativni sistem. Ukoliko Korisnik nakon početka korišćenja usluga UniCredit e-banking, na istom računaru koristi nelicencirane, neprilagođene ili netestirane aplikacije, Banka ne snosi nikakvu odgovornost za neizvršavanje naloga i druge eventualne štetne posledice.
Korisnik je obavezan da obezbedi odgovarajući mobilni uređaj, koji je u mogućnosti da podržava mBanking/mBusiness i mToken aplikacije, ukoliko želi da ugovori ovu uslugu. Ukoliko ne obezbedi odgovarajući mobilni uređaj, neće biti u mogućnosti da koristi uslugu, i svu odgovornost i sve troškove snosi sam.
Korisnik ne može istovremeno da koristi i Token - elektronski uređaj i mToken. U skladu sa navedenim, mora se opredeliti za jednu od ove dve opcije u Zahtevu. Ukoliko Klijent koristi Token – elektronski uređaj, a želi da koristi mToken i zadovoljava uslove iz prethodnog stava, dužan je da Token – elektronski uređaj vrati Banci, ili plati Banci naknadu u slučaju gubitka.

2. HAL e-bank

Ugovaranje korišćenja

U cilju aktiviranja usluge za HAL e-bank, a u zavisnosti od nivoa usluge za koju se opredeli, Korisnik dostavlja Banci popunjena i potpisana sledeća dokumenta:

i. Zahtev, u kom se opredeljuje za ovu vrstu servisa, a kojim Korisnik može da ovlasti određena fizička lica – Krajnje korisnike, da odredi pristup računima, sa naznačenim ovlašćenjima Krajnih korisnika po tim računima.
ii. Generalnu narudžbenicu za izdavanje kvalifikovanih ličnih digitalnih potvrda za privredno društvo
iii. Zahtev za dobijanje digitalne potvrde Krajnjeg korisnika (svako pojedinačno fizičko lice za koje se traži izdavanje pametne kartice).
iv. Izjavu o istinitosti sadržaja digitalne potvrde, svojeručno potpisanu od strane Korisnika (ovlašćenog lica), koji je istovremeno i vlasnik potvrde (na Zahtevu, uz ime ovlašćenog lica neophodno je navesti broj sertifikata na pametnoj kartici koji glasi na Krajnjeg korisnika koji je i vlasnik te digitalne potvrde).
v. Kopija lične karte ovlašćenog lica Korisnika, odnosno izjava da su lični podaci za Krajnjeg korisnika koje je Korisnik dostavio tačni

Ukoliko je Klijent već korisnik HAL e-bank proizvoda za elektronsko bankarstvo preko druge poslovne Banke, Banci dostavlja dokumenta označena pod brojevima i), iii) i v) iz prethodnog stava.

Digitalni sertifikat na pametnoj kartici je neprenosiv i glasi na ime Krajnjeg korisnika.
Na osnovu odobrenog Zahteva i Zahteva za dobijanje digitalne potvrde za Korisnika, Pametne kartice Korisniku uručuje Halcom AD Beograd, u prostorijama Halcom AD Beograd ili putem kuriske službe. Izuzetno, Korisnik može preuzeti pametnu karticu u prostorijama banke, samo u slučaju kada nije u pitanju kvalifikovani sertifikat.
Na osnovu odobrenog Zahteva u kojem je zatraženo izdavanje WEB korisničkog imena za određenog krajnjeg korisnika, Banka uručuje WEB korisničko ime i WEB lozinku krajnjem korisniku tj. licu koje je ovlašćeno za to od strane Koirsnika.

Obaveze i odgovornosti ugovornih strana

Korisnik preuzima obavezu da će se u radu sa HAL e-bank sistemom elektronskog bankarstva, u potpunosti pridržavati važećih zakonskih propisa i uputstva za upotrebu za ovaj softverski proizvod.
Korisnik je dužan da čuva, i preuzima obavezu da od Krajnjeg korisnika zahteva da čuva, pametne kartice kao i tajnost PIN koda, kako ne bi došli u posed trećih lica. Ako Krajnji korisnik sumnja ili ustanovi da je neko saznao njegov PIN kod, potrebno je da ga promeni na način opisan u Korisničkom uputstvu.
Korisnik/ Krajnji korisnik je dužan da čuva PUK kod, kojim je moguće deblokirati pametnu karticu i uneti novi PIN kod u slučaju da je ona blokirana nakon tri neuspešna unosa PIN koda. U slučaju gubitka PUK koda blokiranu karticu je nemoguće otključati i izdati novu. Banka ne snosi nikakvu odgovornost za to.
Korisnik snosi svu štetu nastalu zbog gubitka, neovlašćenog ili neodgovarajućeg korišćenja kartice.
Korisnik je odgovoran za tačnosti svih podataka dostavljenih Banci i obavezan je da joj prijavi svaku promenu tih podataka.
Zabranjeno je kopiranje Digitalnog Sertifikata. Sve štete nastale kopiranjem i pokušajem kopiranja snosi Korisnik.
Korisnik je obavezan da na računarima sa kojih će koristiti usluge HAL e-bank obezbedi licenciran, pravilno konfigurisan operativni sistem (minimalno Winows 7 ili noviji u slučaju jednokorisničke verzije HAL e-bank). Ukoliko Korisnik nakon početka korišćenja usluga HAL e-bank, na istom računaru koristi nelicencirane, neprilagođene ili netestirane aplikacije, Banka ne snosi nikakvu odgovornost za neizvršavanje naloga i druge eventualne štetne posledice.
Korisnici koji su naručili instalaciju i obuku za HAL e-bank u svojim poslovnim prostorijama nakon prijema obaveštenja od Banke o tome da su se stekli uslovi za instalaciju HAL e-bank sistema, u obavezi su da za najviše 15 dana zakažu instalaciju softvera telefonski na brojeve tehničke podrške: (+381 11) 3021 333 ili slanjem poruke putem elektronske pošte na adresu: e-banking@unicreditgroup.rs.
Korisnici koji dobijaju HAL e-bank paket za samostalnu instalaciju nakon prijema obaveštenja od Banke, u obavezi su da u roku ne dužem od 30 dana od dana obaveštavanja, preuzmu paket za HAL e-bank u nekoj od ekspozitura UniCredit Banke.
U slučaju da Korisnik odustane od korišćenja usluga HAL e-bank sistema pre završetka implementacije samog sistema, a nakon obaveštenja od strane Banke da su se stekli tehnički uslovi za implementaciju tog elektronskih servisa, a na način detaljno opisan ranije u tekstu ovih Posebnih uslova, Banka može Korisniku naplatiti naknade u vezi sa instalacijom servisa u skladu sa Tarifom za opšte bankarske usluge. Banka ima pravo, a Korisnik se saglašava da Banka zadrži sredstva koje je u trenutku podnošenja Zahteva naplatila.

3. MultiCash

Ugovaranje korišćenja

U cilju aktiviranja ove usluge elektronskog bankarstva Korisnik je dužan da dostavi Banci popunjena i potpisana sledeća dokumenta:

i. Zahtev za elektronsko bankarstvo, u kome se Korisnik opredeljuje za ovu vrstu usluge elektronskog bankarstva, i navodi Krajnje korisnike koji se ovlašćuju za rad, kao i račune kojima će imati pristup.
ii. Kopija lične karte ovlašćenog lica Korisnika, odnosno izjavu da su lični podaci za Krajnjeg korisnika, koje je Korisnik dostavio, tačni

Odgovornosti i obaveze ugovornih strana

Korisnik se obavezuje da će se u radu sa MultiCash sistemom elektronskog bankarstva, u potpunosti pridržavati važećih zakonskih propisa i uputstava za upotrebu za ovaj softverski proizvod.
Korisnik je dužan da čuva, i preuzima obavezu da od Krajnjeg korisnika zahteva da čuva, Elektronski potpis i lozinku elektronskog potpisa, kao i lozinku za pristup MultiCash aplikaciji i lozinku za komunikaciju sa Bankom, kako oni ne bi došli u posed trećih lica. Ako Korisnik sumnja, ili ustanovi da je neko saznao jednu od navedenih lozinku, potrebno je da je promeni

na način opisan u uputstvu za upotrebu MultiCash softvera.
Korisnik snosi svu štetu nastalu zbog gubitka, neovlašćenog ili neodgovarajućeg korišćenja sigurnosnih sredstava: BPD datoteke i elektronskog potpisa.
Korisnik je dužan da prilikom upotrebe usluga MultiCash poštuje pravila i pridržava se Korisničkog uputstva, koje je sastavni deo programa MultiCash.
Korisnik je odgovoran za tačnosti svih podataka dostavljenih Banci i obavezan je da joj prijavi svaku promenu tih podataka.
Zabranjeno je kopiranje Elektronskog potpisa i BPD datoteke. Svaku štetu nastale kopiranjem i pokušajem kopiranja snosi Korisnik.
Potrebno je da klijent na računarima sa kojih će koristiti usluge MultiCash-a obezbedi licenciran, pravilno konfigurisan operativni sistem (minimalno Windows 2000 Service pack III). Ukoliko Klijent nakon početka korišćenja usluga MultiCash-a, na istom računaru koristi nelicencirane, neprilagođene ili netestirane aplikacije, Banka ne snosi nikakvu odgovornost za neizvršavanje naloga i druge eventualne štetne posledice.
Klijenti koji su naručili instalaciju i obuku za MultiCash u svojim poslovnim prostorijama nakon prijema obaveštenja od Banke o tome da su se stekli uslovi za instalaciju MultiCash sistema, u obavezi su da za najviše 15 dana zakažu instalaciju softvera telefonski na brojeve tehničke podrške: (+381 11) 3021 333 ili slanjem poruke putem elektronske pošte na adresu: e-banking@unicreditgroup.rs.
U slučaju da Korisnik odustane od korišćenja usluga MultiCash sistema pre završetka implementacije samog sistema, a nakon obaveštenja od strane Banke da su se stekli tehnički uslovi za implementaciju tog elektronskih servisa, a na način detaljno opisan ranije u tekstu ovih Posebnih uslova, Banka može Korisniku naplatiti naknade u vezi sa instalacijom servisa u skladu sa Tarifom za opšte bankarske usluge. Banka ima pravo, a Korisnik se saglašava da Banka zadrži sredstva koje je u trenutku podnošenja Zahteva naplatila.

4. MT101

Ugovaranje korišćenja

U cilju aktiviranja ove usluge elektronskog bankarstva Korisnik je dužan da dostavi Banci popunjenu i potpisanu Autorizaciju za izvršavanje MT101 poruka . Korisnik, internacionalni klijent, može ovu uslugu aktivirati i direktno preko Bank Austria potpisivanjem dokumenta Unique Service Level Agreement For MT101.
Banka je ovlašćenja da odbije realizaciju MT101 ukoliko sa zahtevanim SWIFT korisnikom sa čije SWIFT adrese se inicira MT101 poruka nije u mogućnosti da odobri RMA (Relationship Management Application).

5. E-izvod servis

Ugovaranje korišćenja

Korisnik dobija mogućnost korišćenja E-izvod servisa podnošenjem odgovarajućeg Zahteva, a kojim definiše mejl adresu na koju će Banka vršiti dostavu izvoda po računima i drugih obaveštenja u vezi sa poslovnim odnosom Korisnika i Banke.

Obaveze i odgovornosti Banke

Banka je obavezna da računarski evidentira sve postupke Korisnika. Računarski zapis čuva se u skladu sa važećim zakonskim propisima.
Banka zadržava pravo da izmeni sadržaj ili deo sadržaja GWS / HAL e-bank / MultiCash / mBanking / mBusiness / mToken sistema dostupnog Korisniku, bez prethodne najave. O izmeni sadržaja ili dela sadržaja GWS/ HAL e-bank / MultiCash / mBanking / mBusiness / mToken, Banka će naknadno obavestiti Korisnika i saglasno tome mu dostaviti uputstvo.
Banka ne odgovara za smetnje i prekide u telekomunikacionim i teletransmisionim uslugama koje pružaju treća lica, kao ni za greške i štetu nastalu na taj način.
Banka se obavezuje da će Korisniku obezbediti Korisničko uputstvo za korišćenje GWS/ HAL e-bank / MultiCash / mBanking / mBusiness / mToken sistema.
Banka se obavezuje da će Korisniku koji je Zahtevom ugovorio uslugu M-banking, proslediti putem SMS poruke link za preuzimanje i instalaciju aplikacije, kao i aktivacioni kod koji je potreban za pokretanje aplikacije. Zaposleni u ekspozituri će uputiti korisnika na koji način da instalira aplikaciju.
Banka se obavezuje da će Korisniku koji je Zahtevom naručio instalaciju i obuku za korišćenje MultiCash-a i koji je u roku od najviše 30 dana od dana iniciranja Zahteva, pripremio tehničke uslove za uvođenje MultiCash sistema prema podacima navedenim u podnetoj dokumentaciji, obavestiti da su se stekli tehnički uslovi za uvođenje MultiCash sistema slanjem poruke putem elektronske pošte na adresu elektronske pošte Kontakt osobe koja je navedena na Zahtevu. Ukoliko Korisnik nije upisao validnu adresu elektronske pošte, Banka obaveštava o tome Korisnika na broj telefona koji je upisan na Zahtevu.

V. IZVRŠENJE PLATNIH I OSTALIH TRANSAKCIJA

1. Platna transakcija inicirana jednim od servisa elektronskog bankarstva smatra se autorizovanom. Činjenica da je Banka kao korišćenje platnog instrumenta zabeležila korišćenje sredstava za identifikaciju i overu, kojima se pristupa pomoću personalizovanog bezbedonosnog obeležja, biće dovoljna da bi se dokazalo da je Korisnik, odnosno Krajnji korisnik, autorizovao navedenu platnu transakciju, čime Korisnik preuzima na sebe odgovornost za izvršenu navedenu transakciju. Klijent je odgovoran za tačnost svih podataka ispostavljenog naloga za plaćanje.
2. Banka će, neposredno po prijemu naloga za plaćanje, putem istog kanala kojim je nalog za plaćanje primljen, dostaviti Korisniku poruku o uspešnom prijemu naloga. Poruka o uspešnom prijemu naloga za plaćanje ne znači da će nalog za plaćanje biti izvršen, već samo da ga je Banka primila.
3. Banka ispravne naloge za plaćanje izvršava na način i u rokovima koji su dati u Opštim uslovima pružanja platnih usluga fizičkim licima, preduzetnicima i poljoprivrednicima (**u daljem tekstu: OU pružanja platnih usluga**) i Terminskom planu, važećem u trenutku izvršenja platne transakcije.
4. Naloge za plaćanje koji su poslati u Banku nekim od elektronskih platnih instrumenata pre datuma valute izvršenja, Korisnik i Krajnji korisnik mogu opozvati do datuma izvršenja koji je određen važećim Terminskim planom. Nalozi za plaćanje mogu se opozvati korišćenjem istog elektronskog kanala kojim su i dostavljeni Banci, a u skladu sa OU pružanja platnih usluga, osim ukoliko takva mogućnost ne postoji, u kom slučaju će Korisnik opoziv podneti pisanim putem Banci.
5. Banka može odbiti izvršenje naloga za plaćanje u skladu sa OU pružanja platnih usluga.
6. Banka zadržava pravo da ograniči iznos platne transakcije koju korisnik realizuje putem sistema elektronskog/mobilnog bankarstva, a informaciju o ograničenju će učiniti dostupnom korisniku kroz samu aplikaciju koju koristi.
7. Banka ne snosi odgovonost za neizvršenje platne transakcije, ili za pogrešno izvršene platne transakcije putem elektronskih instrumenata, do kojih je došlo zbog netačno unetih podataka u nalogu Korisnika, odnosno Krajnjeg korisnika.

VI. IZVRŠENJE INSTANT TRANSFERA ODOBRENJA NA PRODAJNOM MESTU

1. Banka svojim korisnicima sa kojima je ugovorila korišćenje usluge Mobilnog bankarstva nudi mogućnost izvršenja domaćih platnih transakcija na prodajnom mestu putem instant transfera odobrenja. Platiocima su na raspolaganju dva načina iniciranja instant transfera odobrenja:
    a. prezentovanjem podataka o platiocu putem standardizovane dvodimenzionalne oznake QR koda
    b. preuzimanjem podataka o trgovcu putem standardizovane dvodimenzionalne oznake QR koda
2. Banka će, neposredno po prijemu autorizovanog naloga za instant transfer odobrenja, isti izvršiti u najkraćem mogućem roku ukoliko su ispunjeni uslovi za izvršenje naloga, u okviru raspoloživih sredstava na računu.
3. Banka će Platiocima odmah nakon izvršenog naloga za instant transfer odobrenja, putem poruke mobilnog bankarstva, dostaviti informacije o iznosu i valuti izvršenog zahteva za plaćanje, kao i referentnoj oznaci kojom se identifikuje platna transakcija na prodajnom mestu. Banka će na isti način obavestiti Platioce i u slučaju odbijanja naloga za instant transfer odobrenja.
4. Naloge za instant transfer odobrenja po osnovu Zahteva za plaćanje na prodajnom mestu nije moguće opozvati. Korisnici imaju mogućnost iniciranja Zahteva za povraćaj po osnovu plaćanja na prodajnom mestu. Banka po prijemu Zahteva za povraćaj po osnovu plaćanja na prodajnom mestu pristupa izvršavanju svih neophodnih provera da li je pravilno izvršen zahtev za plaćanje na prodajnom mestu. Ukoliko je na osnovu izvršenih provera utvrđeno da postoji osnov za povraćaj, Banka inicira zahtev za povraćaj sredstava na račun korisnika.

VII. ONEMOGUĆAVANJE PRISTUPA, ODNOSNO GUBITAK ILI BLOKADA SIGURNOSNE OPREME

1. Gubitak, krađu, sumnju na zloupotrebu, ili zloupotrebu sredstava za identifikaciju i overu, sertifikata uskladištenih na sredstvu za identifikaciju i overu, ili personalizovanih bezbednosnih oznaka, saznanje ili sumnju da je neovlašćena osoba saznala personalizovano sigurnosno obeležje, saznanje ili sumnju da je neovlašćenja osoba imala pristup ugovorenom kanalu, Korisnik i Krajnji korisnik su dužni odmah da prijave Banci i da zatraže blokadu pristupa elektronskom bankarstvu.
2. Prijava gubitka ili krađe sredstava za identifikaciju i overu na kojima je pohranjen sertifikat, osnova je za opoziv sertifikata. Banka je dužna da opozove sertifikat nakon prijema prijave.
3. Banka će i bez prijave Korisnika ili Krajnjeg korisnika automatski onemogućiti pristup proizvodu elektronskog bankarstva ako je presonalizovana sigurnosna oznaka uzastopno pogrešno uneta onoliko puta koliko je navedeno u Korisničkom uputstvu.

4. Banka je ovlašćena da bez prijave Korisnika, odnosno Kranjeg korisnika, onemogući pristup pojedinim ili svim proizvodima elektronskog bankarstva, u sledećim slučajevima:
   i. u slučaju sumnje na neovlašćeno korišćenje ili zloupotrebu sredstava za identifikaciju i overu ili personalizovanih sigurnosnih oznaka
   ii. u slučaju da je se proizvod elektronskog bankarstva koristi za prevaru ili zloupotrebu.
5. Banka će unapred obavestiti Korisnika i Kranjeg korisnika o nameravanoj blokadi pristupa i/ili nemogućnosti korišćenja pojedine usluge elektronskog bankarstva, kao i o razlozima takvog postupanja, osim ako je davanje takvog obaveštenja u suprotnosti sa objektivno opravdanim bezbedonosnim razlozima, ili protivno zakonu. Banka nije dužna da unapred obavesti Korisnika i Krajnjeg korisnika o blokadi pristupa elektronskom bankarstvu u slučaju pogrešnog unosa personalizovane bezbedonosne oznake, ili isteka roka važenja sertifikata koji je pohranjen na sredstvu za identifikaciju Krajnjem korisniku. Obaveštenje o nemogućnosti korišćenja proizvoda elektronskog bankarstva ili pojedine usluge, koja je dostupna kroz elektronsko bankarstvo, Banka šalje Korisniku i Krajnjem korisniku putem drugog dostupnog načina.
6. Svi nalozi za plaćanje, koje je Banka primila pre opoziva sertifikata ili blokade pristupa proizvodu elektronskog bankarstva, biće izvršeni.
7. Banka može uz najavu najmanje 24 časa unapred privremeno onemogućiti korišćenje ugovorenih proizvoda elektronskog bankarstva u slučaju promena i nadogradnji informacionog sistema Banke, uključujući sistem njene informacione bezbednosti, ili u slučaju promena ili nadogradnji proizvoda elektronskog bankarstva. Obavestenje o privremenoj nemogućnosti korišćenja proizvoda elektronskog bankarstvaBanka šalje Korisniku i Krajnjem korisniku putem istog proizvoda elektronskog bankarstva, objavom na internet stranici Banke ili na drugi način.

GWS - BusinessNet Professional i Online banking / Mobile banking

Korisnik/ Krajnji korisnik je dužan da gubitak ili krađu tokena ili uređaja na kome je instalirana mBanking / mBusiness aplikacija, bez odlaganja prijavi Banci na broj (+381 11) 3021 333 ili elektronskom poštom na adresu: e-banking@unicreditgroup.rs . Na osnovu dobijenog obaveštenja o gubitku ili krađi tokena, ili uređaja na kome je instalirana mBanking / mBusiness aplikacija, dalje korišćenje tokena ili mBanking / mBusiness aplikacije u raspolaganju sredstvima na računima koji se vode kod Banke će biti onemogućeno, odmah po prispeću obaveštenja, u okviru radnog vremena Službe tehničke podrške, a koje je od ponedeljka – do petka od 09.00h do 17.00h.
Korisnik je dužan da i pisanim putem, u roku od 2 radna dana, obavesti tj. potvrdi Banci gubitak odnosno krađu tokena, ili uređaja na kome je instalirana mBanking / mBusiness aplikacija. Trajno blokiran token se ne može više deblokirati, a troškove ponovnog izdavanja tokena snosi Korisnik. Korisnik će snositi eventualne posledice zloupotrebe izgubljenog ili ukradenog tokena, ili uređaja na kome je instalirana mBanking / mBusiness aplikacija.
U slučaju da Korisnik uzastopno tri puta pogrešno unese PIN kod prilikom korišćenja mBanking / mBusiness aplikacije, dolazi do automatske blokade softerskog tokena, te je neophodno da Korisnik odlaskom u matičnu ekspozituru izvrši ponovnu instalaciju aplikacije.

HAL e-bank sistem

Korisnik/Krajnji korisnik je dužan da gubitak ili krađu pametne kartice bez odlaganja prijavi Banci na broj (+381 11) 3021 333 ili elektronskom poštom na adresu: e-banking@unicreditgroup.rs
Na osnovu dobijenog obaveštenja o gubitku ili krađi kartice/sertifikata, dalje korišćenje pametne kartice/sertifikata u raspolaganju sredstvima na računima koji se vode kod Banke će biti onemogućeno odmah po prispeću obaveštenja, u okviru radnog vremena Službe tehničke podrške od ponedeljka do petka od 09.00h do 17.00h.
Korisnik je dužan da i pisanim putem, u roku od 2 radna dana, obavesti tj. potvrdi Banci gubitak odnosno krađu kartice/ sertifikata. Trajno blokirana kartica/ sertifikat se ne može više deblokirati, a troškove ponovnog izdavanja kartice/ sertifikata snosi Korisnik. Korisnik će snositi eventualne posledice zloupotrebe izgubljene ili ukradene kartice/sertifikata.
U slučaju da Korisnik blokira smart karticu, deblokada je moguća ukoliko Korisnik ima podatke o PUK i PIN kodu, a koji su mu uručeni zajedno sa pametnom karticom za korišćenje HAL e-bank, a sve troškove snosi Korisnik. Banka na pisani zahtev ovlašćenog lica Korisnika podnosi zahtev kod Halcom AD Beograd, za izradu nove pametne kartice sa digitalnim sertifikatom.

VIII. ČUVANJE LIČNIH PODATAKA I POVERLJIVIH INFORMACIJA

Banka kao poverljive čuva sve podatke, činjenice i okolnosti o pojedinom Korisniku kojima raspolaže. Korisnik je saglasan da sve informacije koje je dao Banci, ili ih je Banka saznala prilikom zasnivanja odnosno tokom ugovornog odnosa, Banka moze obrađivati i koristiti u svrhu stvaranje baze klijenata, sprečavanje pranja novca i finansiranje terorizma, istraživanja i otkrivanja prevara u platnom prometu, rešavanja reklamacija i unosa u dokumentaciju koja nastaje radi realizacije prava i obaveza. Banka je dužna da sa navedenim podacima postupa u skladu sa svojom zakonskom obavezom čuvanja tajnosti podataka koje je saznala u poslovanju sa Korisnikom, osiguravajući poverljivost postupanja sa tim podacima i punu zaštitu bankarske tajne na strani svih osoba kojima će biti omogućen pristup zaštićenim podacima, kao i njihovo korišćenje u zakonite svrhe.

IX. ZAVRŠNE ODREDBE

Korisnik je saglasan da Banka ima pravo promene Posebnih uslova i Tarifa za opšte bankarske usluge uz obavezu Banke da u pisanoj formi Korisniku dostavi predlog izmena i dopuna najkasnije dva meseca pre predloženog dana početka primene tih izmena. Korisnik se može saglasiti da predložene izmene i dopune proizvedu pravno dejstvo i pre predloženog dana početka njihove primene. Smatraće se da se Korisnik saglasio sa predlogom izmena i dopuna, ako pre dana početka njihove primene nije obavestio Banku da se ne slaže sa predlogom. Ukoliko Korisnik nije saglasan sa predlogom izmena i dopuna, ima pravo da pre dana početka primene predloženih izmena i dopuna otkaže korišćenje usluga elektronskog bankarstva bez plaćanja naknada i drugih troškova.
U slučaju spora nadležan je sud u skladu sa zakonom.
Za sve što nije predviđeno ovim Posebnim uslovima, primenjuju se OU pružanja platnih usluga i Opšti uslovi poslovanja sa fizičkim licima, preduzetnicima i poljoprivrednicima- Opšti deo.
Ovi Posebni uslovi sačinjeni su u skladu sa Zakonom o platnim uslugama i propisima Republike Srbije i dostupni su na internet prezentaciji Banke www.unicreditbank.rs, kao i u svim ekspozituramа Banke.
Ovi Posebni uslovi sačinjeni na srpskom i engleskom jeziku. U slučaju neusaglašenosti srpske i engleske verzije, verzija na srpskom jeziku će biti merodavna. Banka će savesno postupati prilikom izvršavanja naloga Korisnika i činiti sve što je u njenoj moći radi zaštite interesa Korisnika u svakom pojedinom slučaju.
Odredbe ovih Posebnih uslova stupaju na snagu danom usvajanja od strane Upravnog odbora Banke, a primenjuju se od 01. aprila 2019. godine.

Upravni odbor UniCredit Bank Srbija a.d. Beograd