

**2026-yil 22-sentyabrda KBXKShga kiritilgan qo'shimchalar va
o'zgartirishlarga ilova**

"Jismoniy shaxslar uchun milliy va chet el valyutasidagi bank kartalarini chiqarish va
ularga xizmat ko'rsatish shartnomasini tuzish va bajarish tartibi"ga
11-SONLI ILOVA

**Kontaktsiz to'lov xizmatlaridan foydalanishda Kartalarga xizmat ko'rsatish
qoidalar**

1. Qo'shimcha atamalar va ta'riflar

Kontaktsiz to'lov – Karta egasi tomonidan Token o'rnatilgan Mobil/Aqlli qurilmani o'quvchi to'lov terminaliga yaqinlashtirish yoki tekkizish orqali yoxud internet tarmog'ida to'lov amalga oshirilayotganda To'lov xizmati interfeysi orqali Tokendan foydalangan holda Operatsiyani amalga oshirish usuli.

KBXKSh – Mijoz va Bank o'rtasida "Kapitalbank" ATBda kompleks bank xizmati ko'rsatish qoidalariga Mijozning qo'shilishi orqali tuziladigan Kompleks bank xizmati ko'rsatish shartnomasi bo'lib, unda Shartnomalarni tuzish hamda Masofaviy bank xizmatlari (MBX) doirasida Mijozlarga xizmatlar ko'rsatish shartlari va tartibi belgilanadi. Qoidalar va ularga ilovalar, Bank tariflari, Ommaviy oferta / Qo'shilish shartnomasi, shuningdek, Mijoz tomonidan tegishli tarzda to'ldirilgan Ariza birgalikda Mijoz va Bank o'rtasida tuzilgan BKXSh hisoblanadi;

Shartnoma – Bank va Mijoz o'rtasida BKXSh doirasida tuziladigan, jismoniy shaxslar uchun milliy va chet el valyutasida bank kartalarini chiqarish hamda ularga xizmat ko'rsatish shartnomasini tuzish, ijro etish va bekor qilish tartibini belgilovchi Shartnoma;

Karta egasi (Ega/Mijoz) – amaldagi qonunchilikka, O'zbekiston Respublikasi Markaziy bankining me'yoriy hujjatlariga va Shartnomaga muvofiq Bank tomonidan nomiga Karta chiqarilgan jismoniy shaxs (rezident, norezident).

Karta – ushbu Qoidalar maqsadlari uchun "Kapitalbank" ATBda kompleks bank xizmati ko'rsatish qoidalarida belgilanganidek Plastik/metall va/yoki Virtual karta;

DPAN / Token – To'lov xizmatida shakllantiriladigan, Kartaning shifrlangan rekvizitlari to'plamini ifodalovchi hamda Kartadan jismoniy foydalanmasdan Kontaktsiz to'lovni amalga oshirish uchun qo'llaniladigan Kartaning noyob raqamli ko'rinishi (virtual token).

To'lov xizmati (Raqamli hamyon) – uchinchi tomon Provayderining dasturiy ta'minoti, mobil ilovasi yoki bulutli xizmati bo'lib, u Karta egasiga Kartani qo'shish, Tokenlarni saqlash va ulardan Kontaktsiz to'lovlarni amalga oshirishda foydalanish imkonini beradi.

Xizmat provayderi – tegishli To'lov xizmatining ishlab chiquvchisi va/yoki operatori hisoblangan yuridik shaxs (tizim integratorlari, to'lov tizimlari operatorlari va boshqa uchinchi shaxslar).

Provayder ilovasi – Tokenlarni boshqarish uchun Karta egasining qurilmasiga o'rnatilgan texnik tizim (mobil ilova).

Mobil / Aqlli qurilma – Karta egasining ma'lumotlarni simsiz uzatish (NFC va shunga o'xshash) texnologiyalarini qo'llab-quvvatlaydigan hamda Provayder tomonidan To'lov xizmati bilan ishlash uchun sertifikatlangan har qanday Abonent qurilmasi (smartfon, aqlli soat, planshet, shaxsiy kompyuter, fitnes-bilaguzuk va h.k.).

ODCVM (On-Device Cardholder Verification Method) – biometrik ma'lumotlardan (yuzni, barmoq izini, ko'z to'p pardasini tanish) foydalangan holda yoki qurilma ekranini qulfdan chiqarish paroli/grafik kalitini kiritish orqali bevosita Mobil/Aqlli qurilmaning o'zida Karta egasini verifikatsiya qilish (shaxsini tasdiqlash) usuli.

Qoidalar – kontaktsiz to'lov bo'yicha to'lov xizmatlaridan foydalanishda Kartaga xizmat ko'rsatishning ushbu Qoidalar.

Ushbu Qoidalarda qo'llaniladigan boshqa atamalar va tushunchalar BKXKSh hamda Shartnomadagi bilan bir xil ma'noga ega.

2. Umumiy qoidalar va shartlarning tengligi

- 2.1. Bank va Provayder Karta egalariga Token yaratish va Tokendan foydalangan holda to'lovlarni amalga oshirish imkoniyatini taqdim etadi.
- 2.2. Karta egasi tomonidan Provayderning istalgan Ilovasida ushbu Qoidalarda belgilangan tartibda Token yaratilishi uning ushbu Qoidalar bilan to'liq tanishganini va ularga so'zsiz qo'shilganini (akseptini) anglatadi.
- 2.3. Ushbu Qoidalar Bank tomonidan qo'llab-quvvatlanadigan uchinchi tomon Provayderlarining To'lov xizmatlari orqali to'lovlarni amalga oshirishda Kartalardan foydalanish tartibini tartibga soladi, shuningdek, KBXKSh va Shartnomani to'ldiradi hamda ularning ajralmas qismi hisoblanadi.
- 2.4. Karta egasi To'lov xizmatidan foydalangan holda to'lovlarni ushbu Qoidalar, KBXKSh va Shartnomani inobatga olgan holda amalga oshiradi.
- 2.5. Token faqat amaldagi Kartaga biriktirib chiqarilishi mumkin bo'lib, bunda Bank tomonidan chiqarilgan, amal qilish muddati o'tmagan va Bank tomonidan bloklanmagan faollashtirilgan Karta tushuniladi.
- 2.6. Karta egasi tomonidan Tokendan (DPAN) foydalangan holda amalga oshirilgan Operatsiyalar Karta egasi tomonidan Kartadan foydalangan holda amalga oshirilgan Operatsiyalarga tenglashtiriladi. Bank Tokenlar (DPAN) bo'yicha Operatsiyalarni Avtorizatsiya qilishni Kartalar bo'yicha bo'lgani kabi bir xil shartlarda amalga oshiradi. Tokendan foydalangan holda amalga oshirilgan Operatsiyalar bo'yicha hisob-kitoblar tartibi tegishli Token yaratilgan Karta bo'yicha Operatsiyalar hisob-kitobi tartibi bilan bir xil bo'lib, Bank va Mijoz o'rtasida tuzilgan Shartnoma qoidalari bilan tartibga solinadi.
- 2.7. Karta egasi ushbu Qoidalarni qabul qilar ekan, Tokenni yaratish va undan keyinchalik foydalanish uning yordamida sarflash imkoniyati ta'minlanadigan pul mablag'larini yo'qotishning yuqori xavfi bilan bog'liqligidan xabardor ekanini tasdiqlaydi.
- 2.8. Ushbu Qoidalarni qabul qilish orqali Mijoz Tokendan foydalangan holda Operatsiyalar PIN-kod kiritilmasdan amalga oshirilishini tasdiqlaydi va bunga rozilik bildiradi. Token Karta bo'yicha To'lovni amalga oshirish uchun yetarli identifikatsiya vositasi hisoblanadi.
- 2.9. Face ID, Touch ID, Optic ID qiyofani identifikatsiyalash texnologiyasidan foydalanish yoki Tekshirish kodini kiritish Operatsiyalarni autentifikatsiya qilish va/yoki avtorizatsiya qilish uchun yetarli vosita hisoblanadi, Mijoz bunga to'liq rozi bo'ladi.

3. Tokenni yaratish va faollashtirish tartibi

- 3.1. Bank Karta egalaridan ushbu Qoidalarda ko'rsatilgan tartibda Token yaratish uchun arizalarni qabul qiladi.
- 3.2. Token Karta egasi tomonidan To'lov xizmatida yoki Provayder ilovasidan foydalangan holda, yoki Mobil ilovadan foydalangan holda Karta egasi tomonidan Kartani To'lov xizmatiga qo'shish uchun tegishli ariza yaratish va Bank tomonidan Kartadan To'lov xizmatida foydalanish imkoniyatini qarshi tasdiqlash orqali yaratiladi.
- 3.3. Bankning mobil ilovasi orqali Token yaratish uchun ariza berishda Mijoz ushbu Qoidalar va Provayder shartlari bilan tanishadi. Ushbu Qoidalar bilan tanishganlik ushbu Qoidalarning 3.6-bandida nazarda tutilgan tartibda tasdiqlanadi.
- 3.4. Provayder ilovasida Kartaga Token yaratishda Karta egasi Karta raqamini, kartaning amal qilish muddatini, Karta egasining ismi va familiyasini (Kartada ko'rsatilganidek), Karta xavfsizlik kodini (CVC/CVV - kod) kiritishi, shuningdek Provayderning tegishli shartlariga, shuningdek, ushbu Qoidalariga roziligini tasdiqlashi lozim.
- 3.5. Tokenni yaratish va faollashtirish:

- 3.5.1. Mobil ilovadan foydalangan holda Token yaratish uchun onlayn arizani rasmiylashtirishda - Mobil ilovaning Tasdiqlash oynasida Mobil telefon raqamiga yuborilgan Tekshiruv kodini egasi kiritgandan so'ng.
- 3.5.2. Proвайder Ilovasidan foydalangan holda Token yaratish uchun onlayn arizani rasmiylashtirishda - Bankdan quyidagi tartibda tasdiqnoma olingandan so'ng:
- Karta egasi o'zining mobil telefon raqamiga yuborilgan SMS-kodni (Tekshiruv kodi) oldi va uni Proвайder ilovasining tegishli maydoniga kiritdi, bunda kodni avtomatlashtirilgan tekshirish ijobiy natija berdi.
- 3.6. Foydalanilmayotgan raqamli ma'lumotlarni kamaytirish va xavfsizlikni ta'minlash maqsadida, Bank 30 (o'ttiz) kalendar kun ichida Karta egasi tomonidan yaratilgan, ammo faollashtirilmagan har qanday Tokenlarni avtomatik yoki boshqa tartibda o'chirib tashlash huquqiga ega.
- 3.7. Kartaning amal qilish muddati tugagach, Tokenning amal qilish muddati to'xtatiladi.
- 3.8. Proвайder va/yoki Bank Tokenni chiqarishni rad etish, Tokenni blokirovka qilish/bekor qilish, shu jumladan Token yaratilgan Karta maqomi o'zgarganda, shu jumladan Karta amal qilish muddati tugaganda, Mijoz Kartadan foydalanishni rad etganda va boshqa hollarda rad etish huquqiga ega.

4. Kartalarning hayotiy davrini avtomatlashtirilgan tarzda boshqarish

- 4.1. Kartaning har qanday sababga ko'ra (jumladan, yo'qolishi, o'g'irlanishi, xavfsizligi buzilishi (komprometatsiya) yoki amal qilish muddati tugashi oqibatida) bloklanishi, amal qilishi to'xtatib turilishi, qayta chiqarilishi yoki yopilishi tegishli To'lov tizimlari qoidalariga muvofiq va/yoki tegishli cheklovlar (stop-listlar) mavjud bo'lganda, To'lov xizmatlarida u bilan bog'liq Tokenlarning (DPAN) amal qilishini to'xtatib turishga yoki to'liq o'chirib tashlanishiga olib kelishi mumkin.
- 4.2. Bank alohida To'lov xizmatidagi muayyan Tokenni bloklash, vaqtincha to'xtatib turish yoki o'chirib tashlash huquqiga ega (masalan, muayyan Mobil/Aqlli qurilmaning xavfsizligi buzilganligiga shubha tug'ilganda yoki firibgarlikka qarshi kurashish maqsadida), bunda Kartaning o'zi yoki boshqa qurilmalardagi Tokenlar faol holatda saqlab qolinadi.

5. Huquq va majburiyatlar

5.1. Karta egasi quyidagi huquqlarga ega:

- 5.1.1. To'lov xizmati va/yoki Mobil ilovada (xizmatning mavjudligiga qarab) Karta egasi nomiga chiqarilgan Kartaga Token yaratish va uni qo'shish tashabbusi bilan chiqish;
- 5.1.2. Tokenlarni tegishli Proвайder tomonidan belgilangan qoidalarga muvofiq boshqarish, bunda Mobil ilovadan foydalangan holda Tokenlarni boshqarish Qoidalar, KBXKSh va Shartnomada nazarda tutilgan tartibda amalga oshiriladi;
- 5.1.3. Kartaning bloklanishi/blokdan chiqarilishidan qat'i nazar, Tokenni bloklash (Tokendan foydalangan holda operatsiyalarni amalga oshirishni to'xtatib turish)/Tokenni blokdan chiqarish (Tokendan foydalangan holda operatsiyalarni amalga oshirishni qayta tiklash);
- 5.1.4. Tokenni To'lov xizmatidan o'chirib tashlash;

5.2. Karta egasi quyidagilarga majbur:

- 5.2.1. Tokendan foydalangan holda operatsiyalarni amalga oshirishda, ushbu operatsiya summasi keyinchalik tegishli Token biriktirilgan Karta operatsiyalari bo'yicha hisob-kitob hisobvarag'ida aks ettirilganda ruxsat etilmagan overdraftga/Qarzдорlikka yo'l qo'ymaslik/Mijoz tomonidan Karta bo'yicha belgilangan to'lov limitiga rioya qilish maqsadida rejalashtirilayotgan operatsiya summasini to'g'ri hisobga olish;
- 5.2.2. Token haqidagi ma'lumotlarni (Proвайder ilovasidagi Token identifikatorining oxirgi to'rtta belgisini) saqlash va ushbu ma'lumotlarni Bankning birinchi talabi bilan oq Bankka taqdim etish;

- 5.2.3. Tokenning maxfiyligini ta'minlash hamda Tokendan foydalanishda qo'llaniladigan Mobil qurilmaning yo'qolishining oldini olish bo'yicha yetarli choralarni ko'rish;
- 5.2.4. Tokenlarni faqatgina Karta egasining shaxsan o'zi foydalanadigan Mobil qurilmalarda yaratish;
- 5.2.5. Mobil qurilmaning axborot xavfsizligini ta'minlash bo'yicha yetarli choralarni ko'rish, shu jumladan Mobil qurilma tomonidan "noma'lum" deb belgilangan manbalardan Mobil qurilmaga ilovalarni o'rnatmaslik;
- 5.2.6. Tokendan foydalangan holda to'lovlarni amalga oshirishda Shartnoma va KBXKShda belgilangan Karta bo'yicha amalga oshirilgan operatsiyalarni tasdiqlashga doir majburiyatlarga rioya qilish, shu jumladan slip yoki kassa terminali chekini imzolashdan oldin quyidagi ma'lumotlarning to'g'riligini tekshirish:
- a) "Jami/Total" satrida ko'rsatilgan operatsiya summasi;
 - b) operatsiya valyutasi;
 - v) operatsiya sanasi;
 - g) Karta raqami;
 - d) savdo/xizmat ko'rsatish korxonasi yoki bankning nomi.
- 5.2.7. Token faollashtirilgan To'lov xizmati o'rnatilgan Mobil qurilma yo'qolgan va/yoki uning xavfsizligi buzilgan (komprometatsiya qilingan) taqdirda, Kartani bloklash uchun Shartnoma va KBXKShda belgilangan tartibda Tokenni bloklash maqsadida darhol Bankka murojaat qilish;
- 5.2.8. Mobil qurilmani uchinchi shaxsga topshirishdan yoki Karta egasining ixtiyori bilan Mobil qurilma uning egaligidan/foydalanishidan boshqa tarzda chiqarilishidan oldin Tokenni bloklash uchun Bankka murojaat qilish;
- 5.2.9. Mobil qurilmada uning ishlab chiqaruvchisi tomonidan o'rnatilgan dasturiy ta'minotga o'zgartirishlar kiritish imkonini beruvchi har qanday kengaytirilgan foydalanuvchi huquqlarini olishga olib kelishi mumkin bo'lgan xatti-harakatlarni bajarmaslik.

5.3. Bank quyidagi huquqlarga ega:

- 5.3.1. Tokendan foydalangan holda operatsiyalarni amalga oshirishga limitlar belgilash va bu haqda axborotni Bankning Internet tarmog'idagi rasmiy sayti — www.kapitalbank.uz manzilida joylashtirish orqali Karta egasini xabardor qilish.
- 5.3.2. Tokenni chiqarish/qayta chiqarish/blokdan chiqarishni rad etish, Tokenni bloklash/bekor qilish, shu jumladan undan foydalanib Token yaratilgan Kartaning maqomi o'zgarganda, jumladan Kartaning amal qilish muddati tugaganda, Karta egasi/Mijoz Kartadan foydalanishdan bosh tortganda, Mijoz Qoidalar, KBXKSh va/yoki Shartnomada nazarda tutilgan o'z majburiyatlarini buzganda, shuningdek Bankda Tokendan foydalanilayotgan Mobil qurilmadan uchinchi shaxs foydalanayotgani to'g'risida shubha paydo bo'lganda hamda KBXKSh va Shartnomada nazarda tutilgan boshqa hollarda.

6. Tomonlarning javobgarligi

- 6.1. Karta Karta egasisi Karta rekvizitlari, OTP kodlari va boshqa turdagi Tekshirish kodlarining sir saqlanishi, shuningdek, uchinchi shaxslarning o'z Mobil qurilmasiga kirishini cheklash (uchinchi shaxslar tomonidan Autentifikatsiya/Avtorizatsiya va boshqalar amalga oshirilishidan himoyalani) uchun yakka o'zi va to'liq javobgardir. Kartani Provayder ilovasiga bog'lash uchun bir martalik parol (OTP) / Tekshirish kodini uchinchi shaxslarga berish (shu jumladan, uchinchi shaxslar tomonidan aldov yoki tahdidlar ta'siri ostida sodir etilgan holatlar) Mijoz tomonidan xavfsizlik qoidalarining qo'pol ravishda buzilishi deb baholanadi. Mijoz ushbu bandni buzgan taqdirda, Bank Mijozning Kartasi bo'yicha amalga oshirilgan Operatsiyalar uchun javobgar bo'lmaydi.
- 6.2. Agar Bankda bog'lash jarayoni vakolatsiz shaxs tomonidan yoki firibgarlik maqsadlarida amalga oshirilmoqda deb hisoblashga asoslar mavjud bo'lsa, Bank bir

tomonlarni tartibda Kartani Provayder ilovasida ro'yxatdan o'tkazish imkoniyatini vaqtincha bloklash yoki butunlay rad etish huquqiga ega.

6.3. Agar Kartadan foydalangan holda amalga oshirilgan xarajat Operatsiyasi yuzasidan Mijoz tomonidan Bankka da'vo arizasi (disput) taqdim etilishi orqali e'tiroz bildirilgan bo'lsa va ushbu Operatsiya Mijoz tomonidan ushbu Qoidalarining 5.1-bandi buzilishi oqibatida yuz bergan bo'lsa, Bank To'lovni qaytarishni (Chardjbekni) rad etishga haqli.

6.4. Faollashtirilgan Tokenga ega Mobil qurilmaning yo'qolganligi/xavfsizligi buzilganligi (komprometatsiya) yoki Token rekvizitlarining oshkor bo'lganligi haqida Karta egasi Bankni xabardor qilguniga qadar, Tokendan foydalangan holda amalga oshirilgan barcha operatsiyalar uchun Karta egasi javobgar bo'ladi.

6.5. Bank o'z majburiyatlarini bajarmaganlik yoki lozim darajada bajarmaganlik uchun javobgar bo'lmaydi, agar bunday bajarmaslik/lozim darajada bajarmaslik quyidagi hollarda sodir bo'lgan bo'lsa:

- a) Provayder ilovasi va/yoki Mobil qurilmaning (jumladan, lekin bular bilan cheklanmagan holda, Mobil qurilmaning operatsion tizimi va Mobil qurilmaga o'rnatilgan boshqa dasturiy vositalarning) ishlamasligi yoki noto'g'ri ishlashi oqibatida kelib chiqqan bo'lsa;
 - b) Provayderning xatti-harakatlari va/yoki qarorlari oqibatida kelib chiqqan bo'lsa;
 - c) O'zbekiston Respublikasi davlat hokimiyati organlari / O'zbekiston Respublikasi Markaziy bankining xatti-harakatlari va/yoki qarorlari oqibatida kelib chiqqan bo'lsa;
 - d) Provayderga nisbatan yurisdiksiyasi qo'llaniladigan xorijiy davlatlar davlat hokimiyati organlarining xatti-harakatlari va/yoki qarorlari oqibatida kelib chiqqan bo'lsa, basharti Bank tomonidan bunday bajarmaslik O'zbekiston Respublikasi qonunchiligi talablariga zid bo'lmasa;
 - e) rekvizitlaridan foydalangan holda Token yaratilgan Karta chiqarilgan to'lov tizimining xatti-harakatlari va/yoki qarorlari oqibatida kelib chiqqan bo'lsa;
 - f) Bankning nazorati va javobgarligi doirasidan tashqarida bo'lgan sabablarga ko'ra, shu jumladan uchinchi shaxsning (sotuvchi, tovar, ish, xizmat ko'rsatuvchi va boshqalar) Tokendan foydalangan holda Operatsiyani amalga oshirishni rad etishi, jumladan (lekin bular bilan cheklanmagan holda) u yoki bu davlatda Provayder tomonidan xizmat ko'rsatish qo'llab-quvvatlanmasligi oqibatida kelib chiqqan bo'lsa;
 - j) O'zbekiston Respublikasi qonunchiligi hamda KBXKShda belgilangan yengib bo'lmaydigan kuch (fors-major) holatlari yuzaga kelishi oqibatida yuz bergan bo'lsa.
- 6.6. Provayder ilovasidan foydalanish shartlari va tartibi Bankning javobgarligi va nazorati doirasiga kirmaydi. Karta egasi tomonidan Provayder ilovasidan foydalanish shartlari va tartibiga oid barcha masalalarni Karta egasi Provayder bilan mustaqil ravishda hal qiladi.

7. Boshqa qoidalar

7.1. Ushbu Qoidalar yuzasidan Bank va Karta egasi o'rtasida kelib chiqishi mumkin bo'lgan barcha nizolar KBXKSh va Shartnomada belgilangan tartibda hal etiladi.

7.2. Ushbu Qoidalariga o'zgartirish va/yoki qo'shimchalar kiritish KBXKSh va Shartnomada nazarda tutilgan tartibda amalga oshiriladi.

7.3. Qoidalariga o'zgartirishlar (qo'shimchalar) kiritilgan taqdirda, Bank rejalashtirilayotgan o'zgartirishlar (qo'shimchalar) to'g'risidagi taklifni (ofertani) ular kuchga kirish sanasidan kamida 10 (o'n) taqvimiy kun oldin Bankning Internet tarmog'idagi www.kapitalbank.uz rasmiy veb-saytida tegishli axborotni joylashtirish orqali va/yoki KBXKSh va Shartnomada nazarda tutilgan boshqa usulda Mijozlar/Karta egasilar e'tiboriga yetkazadi.

7.4. Karta egasi ushbu Qoidalariga quyidagi usullarning istalgani orqali rozilik berish (akseptlash) huquqiga ega:

- Bankka ushbu Qoidalar doirasida Topshiriqlar va/yoki Axborot xabarlarini yuborish, shuningdek, Karta egasi tomonidan ushbu Qoidalarining ijrosini davom ettirish niyatidan dalolat beruvchi boshqa harakatlarni amalga oshirish, shu jumladan Bankka ushbu Qoidalar doirasida xizmatlar ko'rsatilishi to'g'risida arizalar taqdim etish orqali;
 - Karta egasining sukuti (harakatsizligi) ko'rinishida Bankning mazkur taklifiga (ofertasiga) rozilik bildirish irodasini ifodalashi orqali; bunda sukut saqlash deganda Bankka bunday o'zgartirish va/yoki qo'shimchalardan yozma ravishda voz kechish arizasining yoki o'zgartirish va/yoki qo'shimchalarni rad etish munosabati bilan Karta egasining Tokendan foydalanishdan yozma ravishda voz kechish arizasining taqdim etilmaganligi tushuniladi;
 - Mijoz tomonidan Qoidalar, ularga kiritilgan o'zgartirish va/yoki qo'shimchalarga rozilik bildirilganining tasdig'i bo'lib Mijoz tomonidan Operatsiyalarning amalga oshirilishi va/yoki Mijoz tomonidan Mobil ilova va/yoki Tokendan foydalanishning davom ettirilishi yoxud Karta egasining Tokendan foydalanishdan yozma ravishda voz kechish arizasining mavjud emasligi hisoblanadi.
- 7.5. Qoidalar Ega tomonidan kafolatli tarzda olinishini ta'minlash maqsadida, Ega kamida 5 (besh) kalendar kunda bir marta mustaqil ravishda yoki vakili orqali Qoidalariga kiritilishi rejalashtirilgan o'zgartirish va qo'shimchalar haqidagi ma'lumotlarni olish uchun Bankka (Bank saytiga) murojaat qilish majburiyatini oladi.
- 7.6. Ushbu Qoidalar bilan tartibga solinmagan barcha masalalar KBXKSh va Shartnoma shartlari (qoidalari) bilan tartibga solinadi.
- 7.7. Agar ushbu Qoidalarining biror-bir bandi biron-bir sababga ko'ra o'z kuchini yo'qotsa, bu Qoidalarining boshqa bandlari haqiqiylikiga daxl qilmaydi.

ПРИЛОЖЕНИЕ №11
*к Порядку заключения и исполнения договора
на выпуск и обслуживание банковских карт в
национальной и иностранной валюте для физических лиц*

**Правила обслуживания Карт при использовании платёжных сервисов
бесконтактной оплаты**

1. Дополнительные термины и определения

Бесконтактная оплата – способ совершения Держателем Карты Операции с использованием Токена путем близкого поднесения или прикосновения Мобильного/Умного устройства с установленным Токеном к считывающему платежному терминалу или при оплате в интернет-пространстве через интерфейс Платежного сервиса.

ДКБО – Договор комплексного банковского обслуживания, заключаемый между Клиентом и Банком посредством присоединения Клиента к Правилам комплексного банковского обслуживания в АКБ «Капиталбанк», в которых оговариваются условия и порядок заключения Договоров и предоставления Клиентам услуг в рамках ДБО. Правила и Приложения к ним, Тарифы Банка, Публичная оферта / Договор присоединения, а также заполненное надлежащим образом Клиентом Заявление, в совокупности являются заключенным между Клиентом и Банком ДКБО;

Договор – Договор, заключаемый между Банком и Клиентом в рамках ДКБО, определяющий порядок заключения, исполнения и расторжения договора на выпуск и обслуживание банковских карт в национальной и иностранной валюте для физических лиц;

Держатель Карты (Держатель/Клиент) - физическое лицо (резидент, нерезидент), на имя которого Банком в соответствии с Действующим законодательством, нормативными документами Центрального банка Республики Узбекистан, Договором, выпущена Карта.

Карта – в целях настоящих Правил под Картой понимаются Пластиковая/металлическая и/или Виртуальная карта, как это определено Правилами комплексного банковского обслуживания в АКБ «Капиталбанк»;

DPAN / Токен – уникальное цифровое представление Карты (виртуальный токен), формируемое в Платежном сервисе, представляющее собой набор зашифрованных реквизитов Карты и используемое для проведения Бесконтактной оплаты без физического использования Карты.

Платежный сервис (Цифровой кошелек) – программное обеспечение, мобильное приложение или облачный сервис стороннего Провайдера, позволяющий Держателю добавлять Карту, хранить Токены и использовать их для совершения Бесконтактной оплаты.

Провайдер сервиса – юридическое лицо (системные интеграторы, операторы платежных систем и иные третьи лица), являющееся разработчиком и/или оператором соответствующего Платежного сервиса.

Приложение Провайдера – техническая система (мобильное приложение), установленная на устройстве Держателя для управления Токенами.

Мобильное / Умное устройство – любое Абонентское устройство Держателя, (смартфон, смарт-часы, планшет, персональный компьютер, фитнес-браслет и др.), поддерживающее технологии беспроводной передачи данных (NFC и аналогичные) и сертифицированное Провайдером для работы с Платежным сервисом.

ODCVM (On-Device Cardholder Verification Method) – метод верификации Держателя карты на самом Мобильном/Умном устройстве с использованием биометрических данных (распознавание лица, отпечатка пальца, сетчатки глаза) или ввода пароля/графического ключа разблокировки экрана устройства.

Правила – настоящие Правила обслуживания Карты при использовании платёжных сервисов по бесконтактной оплате.

Иные термины и определения, используемые в настоящих Правилах, имеют то же значение, что и в ДКБО и Договоре.

2. Общие положения и Равенство условий

2.1. Банк и Провайдер предоставляют Держателям возможность создания Токена и осуществления платежей с использованием Токена.

2.2. Создание Держателем Токена в порядке, установленном настоящими Правилами, в любом Приложении Провайдера означает полное ознакомление и безусловное присоединение (акцепт) Держателя к настоящим Правилам.

2.3. Настоящие Правила регулируют порядок использования Карт при осуществлении платежей через любые поддерживаемые Банком Платежные сервисы сторонних Провайдеров, дополняют и являются неотъемлемой частью ДКБО и Договора.

2.4. Держатель осуществляет платежи с использованием Платежного сервиса с учетом настоящих Правил, ДКБО и Договора.

2.5. Токен может быть выпущен только к действующей Карте, под которой понимается выпущенная Банком активированная Карта с не истекшим сроком действия и не заблокированная Банком.

2.6. Операции, совершенные Держателем с использованием Токена (DPAN), приравниваются к Операциям, совершенным Держателем с использованием Карты. Банк осуществляет Авторизацию Операций по Токенам (DPAN) на тех же условиях, что и по Картам. Порядок расчетов по Операциям, совершенным с использованием Токена, аналогичен порядку расчетов по Операциям с Картой, к которой создан соответствующий Токен, и регулируется положениями заключенного между Банком и Клиентом Договора.

2.7. Держатель, принимая настоящие Правила, подтверждает свою осведомленность о том, что создание и последующее использование Токена связано с повышенными рисками утраты денежных средств, доступ к расходованию которых обеспечивается Токеном.

2.8. Принимая настоящие Правила, Клиент подтверждает и выражает согласие с тем, что Операции с использованием Токена совершаются без ввода ПИН-кода. Токен является достаточным идентификационным средством для осуществления Платежа по Карте.

2.9. Использование технологии распознавания лица Face ID, Touch ID, Optic ID или ввод Проверочного кода является достаточным средством для Аутентификации и/или Авторизации Операций, с чем Клиент полностью соглашается.

3. Порядок создания и активации Токена

3.1. Банк принимает от Держателей заявки на создание Токена в порядке, описанном в настоящих Правилах.

3.2. Токен создается Держателем к Карте в Платежном сервисе либо с использованием Приложения Провайдера, либо с использованием Мобильного приложения путем создания Держателем соответствующей заявки на добавление Карты в Платежный сервис и встречного одобрения Банком возможности использования Карты в Платежном сервисе.

3.3. При подаче заявки на создание Токена через Мобильное приложение Банка, Клиент знакомится с настоящими Правилами и условиями Провайдера. Ознакомление с настоящими Правилами подтверждается в порядке, предусмотренном в п.3.6. настоящих Правил.

3.4. При создании Токена к Карте в Приложении Провайдера Держателю необходимо ввести номер Карты, срок действия карты, имя и фамилию Держателя Карты (как указано на Карте), код безопасности Карты (CVC/CVV – код), а также подтвердить свое согласие с соответствующими условиями Провайдера, а также настоящими Правилами.

3.5. Создание и активации Токена возможно:

3.5.1. при оформлении онлайн-заявления на создание Токена с использованием Мобильного приложения – после ввода Держателем Проверочного кода, направленного на Номер мобильного телефона, в Подтверждающем окне Мобильного приложения.

3.5.2. при оформлении онлайн-заявления на создание Токена с использованием Приложения Провайдера - после получения подтверждения от Банка в следующем порядке:

- Держатель получил SMS-код (Проверочный код), отправленный на Номер мобильного телефона Держателя и ввел его в соответствующее поле Приложения Провайдера, при этом автоматизированная проверка кода дала положительный результат.

3.6. В целях минимизации неиспользуемых цифровых данных и обеспечения безопасности, Банк вправе автоматически или в ином порядке удалять любые созданные, но не активированные Держателем в течение 30 (тридцати) календарных дней Токены.

3.7. При истечении срока действия Карты срок действия Токена прекращается.

3.8. Провайдер и/или Банк вправе отказать в выпуске Токена, заблокировать/аннулировать Токен, в том числе в случае изменения статуса Карты, с использованием которой был создан Токен, включая окончание срока действия Карты, отказа Клиента от использования Карты и в других случаях.

4. Автоматизированное управление жизненным циклом карт

4.1. Блокировка, приостановление действия, перевыпуск или закрытие Карты по любой причине (включая утерю, кражу, компрометацию или истечение срока действия) может повлечь за собой приостановление действия или полное удаление связанных с ней Токенов (DPAN) в Платежных сервисах в соответствии с

правилами применимых Платежных систем и/или при наличии соответствующих ограничений (стоп-листов).

4.2. Банк имеет право заблокировать, временно приостановить или удалить конкретный Токен в отдельном Платежном сервисе (например, при подозрении на компрометацию конкретного Мобильного/Умного устройства или в антифрод-целях), сохраняя при этом саму Карту или Токены на других устройствах активными.

5. Права и обязанности

5.1. Держатель вправе:

5.1.1. инициировать создание и добавление Токена к Карте, выпущенной на имя Держателя, в Платежном сервисе и/или Мобильном приложении (в зависимости от доступности сервиса)

5.1.2. осуществлять управление Токенами в соответствии с правилами, установленными соответствующим Провайдером, при этом управление Токенами с использованием Мобильного приложения осуществляется в порядке, предусмотренном Правилами, ДКБО и Договором;

5.1.3. осуществить блокировку (приостановить совершение операций с использованием Токена/разблокировку Токена (возобновить совершение операций с использованием Токена) независимо от блокировки/разблокировки Карты;

5.1.4. удалить Токен из Платежного сервиса;

5.2. Держатель обязан:

5.2.1. при совершении операций с использованием Токена соизмерять сумму планируемой операции таким образом, чтобы при последующем отражении суммы этой операции по Счету для расчетов по операциям с Картой, к которой выпущен соответствующий Токен, не допустить несанкционированного овердрафта/Задолженности/ соблюдать установленный Клиентом по Карте платежный лимит;

5.2.2. хранить информацию о Токене (последние четыре символа идентификатора Токена в Приложении Провайдера) и предоставлять данную информацию в Банк по первому требованию Банка;

5.2.3. предпринимать достаточные меры по обеспечению конфиденциальности Токена и по предотвращению утраты Мобильного устройства, с помощью которого используется Токен;

5.2.4. создавать Токены на Мобильных устройствах, используемых исключительно Держателем;

5.2.5. предпринимать достаточные меры по обеспечению информационной безопасности Мобильного устройства, в том числе не устанавливать на Мобильное устройство приложения из источников, определенным Мобильным устройством как «неизвестные»;

5.2.6. при совершении платежей с использованием Токена соблюдать установленные Договором и ДКБО обязанности, касающиеся подтверждения совершенных операций по Карте, в том числе, перед подписанием слипа или чека кассового терминала проверять правильность следующих данных:

а) сумму операции, указанную в графе «Итого/Total»;

б) валюту операции;

в) дату операции;

г) номер Карты;

д) название торгового/сервисного предприятия или банка.

5.2.7. в случае утраты и/или компрометации Мобильного устройства, на котором установлен Платежный сервис с активированным Токеном, незамедлительно обратиться в Банк для блокирования Токена в порядке, установленном Договором и ДКБО для блокировки Карты;

5.2.8. до передачи Мобильного устройства третьему лицу либо иному контролируемому Держателем отчуждению Мобильного устройства из своего владения/пользования, обратиться в Банк для блокировки Токена;

5.2.9. не производить действия с Мобильным устройством, которые могут привести к получению любых расширенных прав пользователя с возможностью внесения изменений в установленное производителем Мобильного устройства программное обеспечение.

5.3. Банк вправе:

5.3.1. устанавливать лимиты на совершение операций с использованием Токена и информировать об этом Держателя путем размещения информации на официальном сайте Банка в сети Интернет: www.kapitalbank.uz.

5.3.2. отказать в выпуске/перевыпуске/разблокировании Токена, заблокировать/аннулировать Токен, в том числе в случае изменения статуса Карты, с использованием которой был создан Токен, включая окончание срока действия Карты, отказа Держателя/Клиента от использования Карты, в случае нарушения Клиентом своих обязанностей, предусмотренных Правилами, ДКБО и/или Договором, а также в случае возникновения подозрения у Банка об использовании третьим лицом Мобильного устройства, с помощью которого используется Токен, и в других случаях, предусмотренных в ДКБО и Договоре.

6. Ответственность сторон

6.1. Держатель карты несет единоличную и полную ответственность за сохранение в тайне реквизитов Карты, кодов ОТП и иных видов Проверочных кодов, а также за ограничение доступа третьих лиц к своему Мобильному устройству (для защиты от Аутентификации/ Авторизации и др. третьими лицами). Передача одноразового пароля (ОТП)/ Проверочного кода для привязки Карты к Приложению Провайдера третьим лицам (включая случаи, совершенные под влиянием обмана или угроз со стороны третьих лиц) расценивается как грубое нарушение правил безопасности со стороны Клиента. При нарушении Клиентом настоящего пункта, Банк не несёт ответственности за Операции совершенные по Карте Клиента.

6.2. Банк имеет право в одностороннем порядке временно заблокировать или полностью отказать в возможности регистрации Карты в Приложении Провайдера, если у Банка есть основания полагать, что процедура привязки осуществляется неуполномоченным лицом или в мошеннических целях.

6.3. Банк вправе отказать в Возврате платежа (Чарджбэке) в случае поступления в Банк опротестования совершенной расходной Операции с использованием Карты путем предъявления Клиентом в Банк претензии диспута, если Операция по Карте произошла в случае нарушения Клиентом п.5.1. настоящих Правил.

6.4. До момента извещения Держателем Банка об утрате/компрометации Мобильного устройства с активированным Токеном или о компрометации реквизитов Токена Держатель несет ответственность за все операции, совершенные с использованием Токена.

6.5. Банк не несет ответственность за неисполнение или ненадлежащее исполнение своих обязательств, если такое неисполнение/ненадлежащее исполнение вызвано:

- а) не функционированием или некорректным функционированием Приложения Провайдера и/или Мобильного устройства (включая, но не ограничиваясь, операционную систему Мобильного устройства и иные установленные на Мобильном устройстве программные средства);
- б) действиями и/или решениями Провайдера;
- в) действиями и/или решениями органов государственной власти Республики Узбекистан/ Центрального банка Республики Узбекистан;
- г) действиями и/или решениями органов государственной власти иностранных государств, юрисдикция которых применима к Провайдеру, если такое неисполнение со стороны Банка не противоречит требованиям законодательства Республики Узбекистан;
- д) действиями и/или решениями платежной системы, в рамках которой выпущена Карта, с использованием реквизитов которой создан Токен;
- е) причинами, находящимися вне сферы контроля и ответственности Банка, включая отказ третьего лица (продавца, поставщика товара, работы, услуги и др.) совершить Операцию с использованием Токена, включая (но не ограничиваясь) отсутствием поддержки Провайдера в том или ином государстве;
- ж) возникновением обстоятельств непреодолимой силы, как это определено законодательством Республики Узбекистан и ДКБО.

6.6. Условия и порядок использования Приложения Провайдера находятся вне сферы ответственности и контроля Банка. Все вопросы по условиям и порядку использования Держателем Приложения Провайдера Держатель разрешает с Провайдером самостоятельно.

7. Прочие положения

7.1. Все споры, которые могут возникнуть между Банком и Держателем в связи с настоящими Правилами, разрешаются в порядке, установленном в ДКБО и Договоре.

7.2. Внесение изменений и/или дополнений в настоящие Правила осуществляется в порядке, предусмотренном ДКБО и Договоре.

7.3. В случае внесения изменений (дополнений) в Правила Банк доводит до сведения Клиентов/Держателей предложение (оферту) о планируемых изменениях (дополнениях) не менее чем за 10 (десять) календарных дней до даты вступления их в силу путем размещения соответствующей информации на Сайте Банка в сети Интернет по адресу www.kapitalbank.uz и/или иным способом, предусмотренным в ДКБО и Договоре.

7.4. Держатель вправе согласиться (акцептовать) настоящие Правила любым из следующих способов:

- направление в Банк Поручений и/или Информационных сообщений в рамках настоящих Правил, а также совершение Держателем иных действий, свидетельствующих о намерении Держателя продолжать исполнение настоящих Правил, в том числе представление в Банк заявлений о предоставлении Банком услуг в рамках настоящих Правил.
- выражением воли Держателя на согласие с указанным предложением (офертой) Банка в виде молчания (бездействия) Держателя, под которым понимается

непредставление Банку письменного отказа от таких изменений и/или дополнений либо письменного отказа Держателя от использования Токена в связи с отказом от изменений и/или дополнений.

- Подтверждением согласия Клиента с Правилами, изменениями и/или дополнениями к Правилам является совершение Клиентом Операций, и/или продолжение использования Клиентом Мобильного приложения и/или Токена, либо отсутствие письменного отказа держателя от использования Токена.

7.5. С целью обеспечения гарантированного получения Держателем Правил Держатель обязуется не реже чем один раз в 5 (пять) календарных дней самостоятельно или через представителя обращаться в Банк (на сайт Банка) за сведениями об изменениях и дополнениях, которые планируется внести в Правила.

7.6. Всё, что не урегулировано настоящими Правилами, регулируется положениями ДКБО и Договора.

7.7. Если какое-либо из положений настоящих Правил по какой-либо причине станет недействительным, это не затрагивает действительность других положений Правил.

*to the Procedure for Conclusion and Performance of an Agreement
for the Issuance and Servicing of Bank Cards in
National and Foreign Currency for Individuals*

Rules for Servicing Cards When Using Contactless Payment Services

1. Additional Terms and Definitions

Contactless payment — a method of performing a Transaction by the Cardholder using a Token by closely holding or touching a Mobile/Smart device with an installed Token to a reading payment terminal or when paying in the Internet space through the interface of the Payment Service.

CBSA — the Comprehensive Banking Service Agreement concluded between the Client and the Bank by the Client's accession to the Rules for Comprehensive Banking Services at JSCB "Kapitalbank", which stipulate the terms and procedure for concluding Agreements and providing services to Clients within the framework of remote banking services (RBS). The Rules and Appendices thereto, the Bank's Tariffs, the Public Offer / Accession Agreement, as well as the Application duly completed by the Client, together constitute the CBSA concluded between the Client and the Bank;

Agreement — an Agreement concluded between the Bank and the Client within the framework of the CBSA, determining the procedure for concluding, performing and terminating an agreement for the issuance and servicing of bank cards in national and foreign currency for individuals;

Cardholder (Holder/Client) — an individual (resident, non-resident) in whose name the Card has been issued by the Bank in accordance with the Applicable Legislation, regulatory documents of the Central Bank of the Republic of Uzbekistan, and the Agreement.

Card — for the purposes of these Rules, Card means a Plastic/metal and/or Virtual card, as defined by the Rules for Comprehensive Banking Services at JSCB "Kapitalbank";
DPAN / Token — a unique digital representation of the Card (virtual token) generated in the Payment Service, which is a set of encrypted Card details and is used for Contactless payment without physical use of the Card.

Payment Service (Digital Wallet) — software, a mobile application or a cloud service of a third-party Provider that allows the Cardholder to add the Card, store Tokens and use them to make Contactless payments.

Service Provider — a legal entity (system integrators, payment system operators and other third parties) that is the developer and/or operator of the relevant Payment Service.

Provider Application — a technical system (mobile application) installed on the Cardholder's device for managing Tokens.

Mobile / Smart device — any Subscriber device of the Cardholder (smartphone, smart watch, tablet, personal computer, fitness bracelet, etc.) supporting wireless data transmission technologies (NFC and similar) and certified by the Provider for operation with the Payment Service.

ODCVM (On-Device Cardholder Verification Method) — a method of verifying the cardholder on the Mobile/Smart device itself using biometric data (face recognition, fingerprint, retina) or entering a password/graphic key to unlock the device screen.

Rules — these Rules for Servicing Cards When Using Contactless Payment Services.

Other terms and definitions used in these Rules have the same meaning as in the CBSA and the Agreement.

2. General Provisions and Equality of Conditions

- 2.1. The Bank and the Provider provide Cardholders with the possibility of creating a Token and making payments using the Token.
- 2.2. Creation by the Cardholder of a Token in the manner established by these Rules in any Provider Application means the Cardholder's full familiarization with and unconditional accession (acceptance) to these Rules.
- 2.3. These Rules regulate the procedure for using Cards when making payments through any Payment Services of third-party Providers supported by the Bank, supplement and are an integral part of the CBSA and the Agreement.
- 2.4. The Cardholder makes payments using the Payment Service subject to these Rules, the CBSA and the Agreement.
- 2.5. A Token may be issued only for a valid Card, which means an activated Card issued by the Bank with an unexpired validity period and not blocked by the Bank.
- 2.6. Transactions performed by the Cardholder using the Token (DPAN) are equated to Transactions performed by the Cardholder using the Card. The Bank authorizes Transactions on Tokens (DPAN) on the same terms as on Cards. The settlement procedure for Transactions performed using the Token is similar to the settlement procedure for Transactions with the Card to which the corresponding Token was created, and is governed by the provisions of the Agreement concluded between the Bank and the Client.
- 2.7. By accepting these Rules, the Cardholder confirms awareness that the creation and subsequent use of the Token is associated with increased risks of loss of funds, access to which is provided by the Token.
- 2.8. By accepting these Rules, the Client confirms and agrees that Transactions using the Token are performed without entering a PIN code. The Token is a sufficient identification means for making a Payment by Card.
- 2.9. Use of Face ID, Touch ID, Optic ID recognition technology or entry of a Verification code is a sufficient means for Authentication and/or Authorization of Transactions, with which the Client fully agrees.

3. Procedure for Creating and Activating a Token

- 3.1. The Bank accepts applications from Cardholders for Token creation in the procedure described in these Rules.
- 3.2. The Token is created by the Cardholder for the Card in the Payment Service either using the Provider Application or using the Mobile application by the Cardholder creating the corresponding application to add the Card to the Payment Service and the Bank's counter-approval of the possibility of using the Card in the Payment Service.
- 3.3. When submitting an application for Token creation through the Bank's Mobile application, the Client familiarizes himself with these Rules and the Provider's terms. Familiarization with these Rules is confirmed in the manner provided for in clause 3.6 of these Rules.
- 3.4. When creating a Token for a Card in the Provider Application, the Cardholder must enter the Card number, card expiry date, name and surname of the Cardholder (as indicated on the Card), the Card security code (CVC/CVV code), and also confirm consent to the relevant terms of the Provider, as well as these Rules.
- 3.5. Creation and activation of the Token is possible:
 - 3.5.1. when completing an online application for Token creation using the Mobile application — after the Cardholder enters the Verification code sent to the Mobile phone Number in the Confirmation window of the Mobile application.

- 3.5.2. when completing an online application for Token creation using the Provider Application — after receiving confirmation from the Bank in the following procedure:
- The Cardholder received an SMS code (Verification code) sent to the Cardholder's Mobile phone Number and entered it in the corresponding field of the Provider Application, and the automated code verification returned a positive result.
- 3.6. In order to minimize unused digital data and ensure security, the Bank has the right to automatically or otherwise delete any Tokens created but not activated by the Cardholder within 30 (thirty) calendar days.
- 3.7. Upon expiry of the Card's validity period, the Token's validity period terminates.
- 3.8. The Provider and/or the Bank has the right to refuse issuance of a Token, block/annul a Token, including in the event of a change in the status of the Card with which the Token was created, including expiry of the Card, the Client's refusal to use the Card, and in other cases.

4. Automated Card Lifecycle Management

- 4.1. Blocking, suspension, reissuance or closure of the Card for any reason (including loss, theft, compromise or expiry) may entail suspension or complete deletion of the Tokens (DPAN) associated with it in Payment Services in accordance with the rules of the applicable Payment systems and/or in the presence of relevant restrictions (stop-lists).
- 4.2. The Bank has the right to block, temporarily suspend or delete a specific Token in a separate Payment Service (for example, if compromise of a specific Mobile/Smart device is suspected or for anti-fraud purposes), while keeping the Card itself or Tokens on other devices active.

5. Rights and Obligations

5.1. The Cardholder has the right to:

- 5.1.1. initiate the creation and addition of a Token to the Card issued in the Cardholder's name in the Payment Service and/or Mobile application (depending on service availability)
- 5.1.2. manage Tokens in accordance with the rules established by the relevant Provider, while management of Tokens using the Mobile application is carried out in the procedure provided for by the Rules, the CBSA and the Agreement;
- 5.1.3. block (suspend transactions using the Token)/unblock the Token (resume transactions using the Token) independently of blocking/unblocking the Card;
- 5.1.4. delete the Token from the Payment Service;

5.2. The Cardholder is obliged to:

- 5.2.1. when performing transactions using the Token, commensurate the amount of the planned transaction so that, upon subsequent reflection of the amount of this transaction on the Account for settlements on transactions with the Card to which the corresponding Token was issued, unauthorized overdraft/Debt is not allowed / observe the payment limit established by the Client on the Card;
- 5.2.2. keep information about the Token (the last four characters of the Token identifier in the Provider Application) and provide this information to the Bank upon the Bank's first request;
- 5.2.3. take sufficient measures to ensure confidentiality of the Token and to prevent loss of the Mobile device by means of which the Token is used;
- 5.2.4. create Tokens on Mobile devices used exclusively by the Cardholder;
- 5.2.5. take sufficient measures to ensure information security of the Mobile device, including not installing on the Mobile device applications from sources designated by the Mobile device as "unknown";

5.2.6. when making payments using the Token, comply with the obligations established by the Agreement and the CBSA concerning confirmation of completed transactions on the Card, including, before signing the slip or cash terminal receipt, checking the correctness of the following data:

- a) the transaction amount indicated in the “Total” column;
- b) the currency of the transaction;
- c) the date of the transaction;
- d) the Card number;
- e) the name of the merchant/service enterprise or bank.

5.2.7. in the event of loss and/or compromise of the Mobile device on which the Payment Service with an activated Token is installed, immediately contact the Bank to block the Token in the procedure established by the Agreement and the CBSA for blocking the Card;

5.2.8. before transferring the Mobile device to a third party or other alienation of the Mobile device from his possession/use controlled by the Cardholder, contact the Bank to block the Token;

5.2.9. not perform actions with the Mobile device that may lead to obtaining any extended user rights with the ability to make changes to the software installed by the manufacturer of the Mobile device.

5.3. The Bank has the right to:

5.3.1. establish limits for transactions using the Token and inform the Cardholder thereof by posting information on the Bank’s official website on the Internet:
www.kapitalbank.uz.

5.3.2. refuse issuance/reissuance/unblocking of a Token, block/annul a Token, including in the event of a change in the status of the Card with which the Token was created, including expiry of the Card, refusal of the Cardholder/Client to use the Card, in the event of violation by the Client of its obligations provided for by the Rules, the CBSA and/or the Agreement, as well as in the event the Bank suspects use by a third party of the Mobile device by means of which the Token is used, and in other cases provided for in the CBSA and the Agreement.

6. Liability of the Parties

6.1. The cardholder bears sole and full responsibility for keeping secret the Card details, OTP codes and other types of Verification codes, as well as for restricting third parties’ access to his Mobile device (to protect against Authentication/Authorization, etc. by third parties). Transfer of a one-time password (OTP)/Verification code for linking the Card to the Provider Application to third parties (including cases committed under the influence of deception or threats from third parties) is regarded as a gross violation of security rules by the Client. If the Client violates this clause, the Bank is not liable for Transactions performed on the Client’s Card.

6.2. The Bank has the right to unilaterally temporarily block or completely refuse the possibility of registering the Card in the Provider Application if the Bank has grounds to believe that the linking procedure is being carried out by an unauthorized person or for fraudulent purposes.

6.3. The Bank has the right to refuse a payment Return (Chargeback) if a protest of a completed expenditure Transaction using the Card is received by the Bank by the Client filing a dispute claim with the Bank, if the Card Transaction occurred in the event of the Client’s violation of clause 5.1 of these Rules.

6.4. Until the Cardholder notifies the Bank of the loss/compromise of the Mobile device with an activated Token or of the compromise of the Token details, the Cardholder is liable for all operations performed using the Token.

6.5. The Bank is not liable for non-performance or improper performance of its obligations if such non-performance/improper performance is caused by:

- a) non-functioning or incorrect functioning of the Provider Application and/or Mobile device (including, but not limited to, the operating system of the Mobile device and other software installed on the Mobile device);
- b) actions and/or decisions of the Provider;
- c) actions and/or decisions of state authorities of the Republic of Uzbekistan/ the Central Bank of the Republic of Uzbekistan;
- d) actions and/or decisions of state authorities of foreign states whose jurisdiction is applicable to the Provider, if such non-performance by the Bank does not contradict the requirements of the legislation of the Republic of Uzbekistan;
- e) actions and/or decisions of the payment system within which the Card was issued, using the details of which the Token was created;
- f) reasons beyond the Bank's control and responsibility, including refusal of a third party (seller, supplier of goods, works, services, etc.) to perform a Transaction using the Token, including (but not limited to) lack of Provider support in a particular state;
- g) occurrence of force majeure circumstances, as defined by the legislation of the Republic of Uzbekistan and the CBSA.

6.6. The terms and procedure for using the Provider Application are outside the sphere of responsibility and control of the Bank. The Cardholder resolves all issues regarding the terms and procedure for the Cardholder's use of the Provider Application independently with the Provider.

7. Miscellaneous Provisions

7.1. All disputes that may arise between the Bank and the Cardholder in connection with these Rules are resolved in the procedure established in the CBSA and the Agreement.

7.2. Amendments and/or additions to these Rules are made in the procedure provided for in the CBSA and the Agreement.

7.3. In the event of amendments (additions) to the Rules, the Bank brings to the attention of Clients/Cardholders the proposal (offer) on the planned amendments (additions) no less than 10 (ten) calendar days before the date of their entry into force by posting the relevant information on the Bank's Website on the Internet at www.kapitalbank.uz and/or in another manner provided for in the CBSA and the Agreement.

7.4. The Cardholder has the right to agree (accept) these Rules in any of the following ways:

- sending to the Bank Orders and/or Information messages within the framework of these Rules, as well as the Cardholder performing other actions indicating the Cardholder's intention to continue performing these Rules, including submitting to the Bank applications for the Bank to provide services within the framework of these Rules.
- expression of the Cardholder's will to agree with the specified proposal (offer) of the Bank in the form of silence (inaction) of the Cardholder, which means failure to submit to the Bank a written refusal of such amendments and/or additions or a written refusal of the Cardholder to use the Token in connection with refusal of the amendments and/or additions.
- Confirmation of the Client's consent to the Rules, amendments and/or additions to the Rules is the Client's performance of Transactions, and/or continuation of the Client's use of the Mobile application and/or Token, or absence of a written refusal of the holder to use the Token.

7.5. In order to ensure guaranteed receipt by the Cardholder of the Rules, the Cardholder undertakes, not less than once every 5 (five) calendar days, independently or through a representative, to contact the Bank (the Bank's website) for information on amendments and additions planned to be made to the Rules.

7.6. Everything that is not regulated by these Rules is governed by the provisions of the CBSA and the Agreement.

7.7. If any provision of these Rules for any reason becomes invalid, this does not affect the validity of other provisions of the Rules.