типовая форма утверждена

Правлением АО "Tengri Bank"
(протокол заседания от
"25"декабря 2018 года № 74)

Үшінші тұлғалардың ақпараттық жүйелері арқылы электрондық банктік қызмет көрсету туралы ереже

Осы Үшінші тұлғалардың ақпараттық жүйесі арқылы электрондық банктік қызмет көрсету туралы ереже (бұдан әрі – Ереже) қашықтықтан банктік қызмет көрсету аясында "Tengri Bank" АҚ (бұдан әрі – Банк) мен үшінші тұлғалар (бұдан әрі – Серіктес) арасындағы қарым-қатынастарды, сондай-ақ осы Шартқа сәйкес Серіктестің ақпараттық жүйелері арқылы заңды тұлғаларға және жеке кәсіпкерлерге электрондық банктік қызмет көрсету рәсімін, оның жалпы талаптарын және оған қойылатын шектеулерді реттейді. Осы Ереже Қазақстан Республикасының заңнамасына және Банктің ішкі нормативтік құжаттарына (бұдан әрі – ішкі құжаттар) сәйкес әзірленген.

1 бөлім. ЖАЛПЫ ЕРЕЖЕЛЕР

1. Осы Ереже Банк пен Серіктес арасында жасалған Серіктеспен аутсорсинг шартының ажырамас бөлігі болып табылады. Серіктес Аутсорсинг шартын жасау арқылы осы Ережеге қосылады және:
   1) осы Ережені алғанын, танысқанын және онымен сөзсіз келісетінін;
   2) осы Ережені және Қазақстан Республикасының қолданыстағы заңнамасының талаптарын сақтайтынын және оларды басшылыққа алатынын растайды.
2. Осы Ережеде Қазақстан Республикасының заңнамасында және ішкі құжаттарда көзделген анықтамалар, сондай-ақ келесі ұғымдар мен шартты белгілер қолданылады:
   1) пікірталас, пікірталасты жағдай немесе даулы жағдай – Банк Клиентінің ресми арналар арқылы жіберген өз тапсырмаларының орындалу фактісімен немесе оның мазмұнымен келіспейтіндігін білдіретін электрондық банктік қызмет көрсету мәселелері жөніндегі жағдайлар;
   2) Аутсорсинг шарты (бұдан әрі Шарт) – Серіктестің ақпараттық арналары арқылы Банк Клиенттеріне электрондық банктік қызмет көрсету үшін Серіктес пен Банк арасында жасалған шарт;
   3) қорғалған байланыс арнасы – Банк пен Серіктес арасында бір-біріне берілетін мәліметтер мен деректерді тыңдауға және өзгертуге мүмкіндік бермейтін IPSec технолгиясын қолдана отырып, Банк пен Серіктес арасында ұйымдастырылған байланыс арнасы;
   4) құпия ақпарат – банктік, коммерциялық құпия және заңмен қорғалатын кез келген ақпарат, оның ішінде жеке деректер.
   5) Клиент – Банкпен жасалған шарттық қарым-қатынастар негізінде Серіктестің жүйесі мен функциялары арқылы электрондық банктік қызметтерді пайдаланатын заңды тұлға / өкілеттік / жеке кәсіпкер / жеке нотариус / жеке сот орындаушысы / адвокат және кәсіби медиатор;
   6) ашық (жария) кілт – куәландырушы орталық құрастырған және кез келген тұлға қол жеткізе алатын, электрондық цифрлық қолтаңба мен электрондық құжаттардың түпнұсқалығын растауға арналған электрондық цифрлық символдардың кезектілігі;

7) Серіктес – Банк Клиенттеріне қашықтықтан банктік қызметтер көрсетуді іске асыру мақсатында Банкпен ынтымақтастық жасайтын заңды тұлға / жеке кәсіпкер;

8) тіркеу куәлігі – электрондық цифрлық қолтаңбаның Қазақстан Республикасының заңнамасында белгіленген талаптарға сәйкестігін растау үшін куәландырушы орталық беретін электрондық түрдегі құжат;

9) техникалық құжаттама – Банк пен Серіктестің техникалық жүйелерінің техникалық өзара әрекет етуі үшін қажетті құжаттама немесе кез келген техникалық ақпарат. Құжаттама api.tengribank.kz интернет-ресурсына орналастырылады;

10) куәландырушы орталық – электрондық цифрлық қолтаңба ашық кілтінің электрондық цифрлық қолтаңба жабық кілтіне сәйкестігін куәландыратын, сондай-ақ тіркеу куәлігінің шынайылығын растайтын жеке тұлға;

11) электрондық банктік қызметтер –транзакциялық (төлем) қызметтер және ақпараттық банктік қызметтер алу үшін Клиенттің жүйе арқылы өз банктік шотына қол жеткізуімен байланысты Клиенттің электрондық құжаттарды жасау түріндегі қызметтер.

12) электрондық цифрлық қолтаңба (бұдан әрі – ЭЦҚ) – электрондық цифрлық қолтаңба құралдарымен жасалған және электрондық құжаттың, оның тиістілігін және мазмұнының өзгермейтіндігін растайтын электрондық цифрлық символдар жиынтығы. ЭЦҚ электрондық құжаттың авторын және/немесе құжатты беру жүзеге асырылған аутентификациялау құралын анықтауға және қол қойылған сәттен бастап құжаттың өзгертілмегенін растауға мүмкіндік береді.

3. Серіктес Банкке Серіктестің ақпараттық жүйелеріне электрондық банктік қызметтерді ендіру бойынша қызмет көрсетеді және Банк Клиенттерінің оған қол жеткізуін қамтамасыз етеді.

4. Серіктестің ақпараттық жүйелері арқылы Клиентке электрондық банктік қызмет көрсету тәртібі Заңды тұлғалар мен жеке кәсіпкерлерге электрондық банктік қызмет көрсету ережесінде ретке келтірілген.

5. Серіктестің ақпараттық жүйелеріне орналастырылған электрондық банктік қызметтер тізбесі:

1) ақпараттық банктік қызметтер (Клиенттің банктік шоттары бойынша ақша қалдықтары және олардың қозғалысы туралы ақпарат беру, және, төлемдер мен аударымдар тарихын қарап шығу, банктік шот нөмірі және валютасы туралы ақпарат, Клиенттің депозиттері, кредиттері, кепілдіктері мен басқа да шарттары туралы ақпарат, сыйақы мөлшерлемелері, ай сайынғы төлем мөлшері, шарттардың электрондық көшірмелерін қарау, депозиттер, кредиттер, кепілдіктер бойынша жүргізілген төлемдер және т.т., бөлімшелердің мекенжайлары, валюта бағамдары, Банктің өнімдері мен акциялары туралы ақпарат беру);

2) транзакциялық (төлемдік) банктік қызметтер (Клиенттердің ағымдағы шоттарынан төлемдер мен аударымдарды, бюджетке төленетін төлемдерді, қызметті жеткізіп берушілердің пайдасына төлемдерді, қолма қол ақшасыз айырбастауды жүзеге асыру);

6. Электрондық банктік қызметтердің тізбесі түпкілікті болып табылмайды және ол Банктің қалауы бойынша толықтырылуы мүмкін. Тізбеге өзгерту енгізілгені туралы хабарлама Банктің (www.tengribank.kz) интернет-ресурсына ақпарат орналастыру арқылы жүргізіледі.

7. Серіктестің ақпараттық жүйесі жүйелі-мәнді, мәнді немесе өзге де төлем жүйесіне жатпайды, ал Серіктес төлем ұйымы болып табылмайды. Серіктес заңнамада төлем ұйымдары үшін белгіленген критерийлерге, ал оның ақпараттық жүйесі жүйелі-мәнді, мәнді немесе өзге де төлем жүйесіне сәйкес келген жағдайда, Серіктес Шарттың талаптарын бұзған болып саналады, Шарт бұзылады және Серіктестің Банк пен Клиентті хабардар еткеніне/ етпегеніне қарамастан осындай сәйкестіктер анықталған күннен бастап Ереже Серіктеске қатысты қолданылмайды. Серіктес Банк пен Клиентке келтірілген залалды толық көлемде өтейді және өзінің ақпараттық жүйесі аясында деректерді қайтару және Банк пен Клиенттің жүйесіне кіруді жабу бойынша қажетті шараларды жүргізеді.

8. Ереженің қандай да бір талаптары заңнамада көзделген негіздер бойынша қолданыста болуын тоқтатқан жағдайда, Ереженің қалған талаптары қолданылуын жалғастырады.

9. Серіктес Шартқа қол қою арқылы Банктің Шартқа және/немесе Ережеге бір жақты тәртіппен өзгерістер мен толықтырулар енгізуіне және жаңа редакциядағы Шартты және/немесе Ережені немесе Шартқа және/немесе Ережеге енгізілген өзгерістер мен толықтыруларды www.tengribank.kz. мекенжайы бойынша Банктің интернет-ресурсына орналастыруына өзінің келісімін береді.

2 бөлім. ЭЛЕКТРОНДЫҚ БАНКТІК ҚЫЗМЕТТЕРДІ ОРНАЛАСТЫРУ ТӘРТІБІ

10. Серіктестің ақпараттық жүйелерінде электрондық банктік қызметтерді көрсетуді бастау үшін келесі іс-шаралар орындалуы тиіс:
    1) Банк пен Серіктес арасында Шарт жасау;
    2) Серіктестің ақпараттық жүйелерін Қашықтықтан банктік қызмет көрсету жүйесіне қосу жөнінде техникалық жұмыстар жүргізу;
    3) Банкте Серіктестің есеп шотын ашу;
    4) Банкке Серіктестің ашық кілтін беру;
    5) Банк пен Серіктес арасында қорғалған байланыс арнасын ұйымдастыру;
    6) екі тараппен де Серіктестің "Ақпараттық жүйелерде электрондық банктік қызметтермен жұмыс кезіндегі ақпараттық қауіпсіздік ережелері" атты құжатын келісу;
    7) қосу схемасының Ішкі нормативтік құжаттардың ақпараттық қауіпсіздік саласындағы талаптарына сәйкестігі туралы ақпараттық қауіпсіздік бөлімшесінің тұжырымдамасын алу.

    Серіктес Банкпен жасалған шарттарды орындау мақсатында жаңа Пайдаланушыны Серіктестің ақпараттық жүйесіне тіркеу кезінде Пайдаланушының жеке деректерін (оның ішінде, трансшекаралық) жинауға, өңдеуге және Банкке беруге Пайдаланушының/ Клиенттің жазбаша келісімін алғандығына кепілдік береді.
11. Электрондық банктік қызметтер көрсетуді бастар алдында Серіктес өзінің ақпараттық жүйелері арқылы тек өзінің банктік шоттары мен өнімдерін ғана басқара алады. Банктің Клиенттеріне электрондық банктік қызметтер көрсету үшін Клиент Банкке Серіктестің ақпараттық жүйелері арқылы электрондық банктік қызметтер алуға келісетіні туралы өтініш беруі тиіс. Өтініштің нысаны мен оны беру тәртібі Заңды тұлғалар мен жеке кәсіпкерлерге электрондық банктік қызмет көрсету туралы ережеде ретке келтірілген.
12. Жүйеге қосу бойынша техникалық жұмыстарды жүргізу үшін Банк Шартқа қол қойылғаннан кейін Серіктеске техникалық құжаттарға қол жеткізу мүмкіндігін береді.
13. Банк өзгерістер енгізгенге дейін 15 (он бес) күнтізбелік күн бұрын бұл жөнінде Серіктесті хабардар ете отырып, өз қалауы бойынша техникалық құжаттамаға және қосу рәсіміне өзгерістер енгізу құқығын өзіне қалдырады.
14. Банк пен Серіктес арасында ақпаратпен алмасу Банк тарапынан, сондай-ақ Серіктес тарапынан да әрбір хабарға ЭЦҚ қою арқылы қорғалған арналар бойынша жүзеге асырылады.
15. Банк пен Серіктес әрбір сұрату және жауап үшін куәландырушы орталықты пайдалана отырып, ЭЦҚ және ашық кілттердің легитимділігін тексеруге және осындай тексерулердің қорытындысы жазылған журналдарды кемінде 5 жыл сақтауға міндетті.
16. Серіктестің ақпараттық жүйелері арқылы Клиенттердің сұратуларына қол қою тәртібі Электрондық банктік қызметтер көрсету тәртібінде ретке келтірілген.
17. Қорғалған арналар арқылы алынған және Серіктестің дұрыс ЭЦҚ бар хабарлардың Серіктестің қолы қойылған және мөрі басылған қағаз тасымалдаушыдағымен маңызы бірдей болып табылады.
18. Серіктестен алынған хабарлар Банктің ақпараттық жүйесінде оның дұрыстығын анықтау үшін жүргізілген барлық тексеруден кейін алынған болып саналады. Дұрыстығын тексеру деген ЭЦҚ және хабар пішімінің дұрыстығын тексеруді білдіреді.

3 тарау. ПІКІРТАЛАС ЖАҒДАЙЛАРЫН ШЕШУ ТӘРТІБІ ЖӘНЕ ХАБАРЛАМАЛАР

19. Ақпараттық жүйелерге қызмет көрсету процестерінде нәтижелі байланыс орнату және Банктің ақпараттық жүйелерінің жұмысы туралы хабарландыру үшін Серіктес Банкке Серіктестің Қолдау қызметінің байланыс деректерін хабарлайды.

20. Серіктес Банкті ол арқылы/оған Банктің электрондық банктік қызметтері ұсынылатын өзінің ақпараттық жүйелерінің тұрып қалған барлық жағдайлары туралы осы факт анықталған сәттен бастап бір сағаттан кешіктірмей Банктің Қолдау қызметі мекенжайына хабарлама жіберу арқылы хабардар етуге міндетті.
21. Серіктес әркез Серіктестің ақпараттық жүйелерін пайданатын Банк Клиенттерін Банктің электрондық банктік қызметтерін ұсынудың тоқтатылу фактісі туралы тоқтатылу фактісі анықталған сәттен бастап бір сағаттан кешіктірмей Банкке растау берумен SMS түрінде хабардар етуге міндетті.
22. Пікірталас жағдайлары туындаған кезде Серіктес Банкті наразылықтың негізді екенін растайтын құжаттарды (бар болса) қосу арқылы Клиент пікірталастық жағдайды анықтаған сәттен бастап 15 (он бес) күнтізбелік күн ішінде хабардар етеді. Банктің Клиенттен даулы жағдай туралы осындай өтінішті көрсетілген мерзім ішінде алмауы жүргізілген төлемнің немесе өзге операцияның дұрыстығын растау болып саналады.
23. Банк алынған өтініштің негізінде заңсыз төлемдер тәуекелін төмендету мақсатында пікірталастық жағдайды тексеруді жүргізген кезде, Банк Клиент мүддесі үшін өз қалауы бойынша Серіктестің ақпараттық жүйелері арқылы электрондық банктік қызметтерді ұсынуды тоқтата тұруға дейін Клиенттің шығындары мен шығыстарының алдын алу үшін шара қабылдауға құқылы.
24. Клиенттердің төлемдерімен пікірталастық жағдайларды шешу тәртібі толығырақ Заңды тұлғаларға және жеке кәсіпкерлерге электрондық банктік қызметтерді ұсыну ережелерінде келтірілген.
25. Хабарламалардың барлық түрлерін Серіктес Банктің Қолдау қызметіне электрондық түрде api@tengribank.kz мекен-жайы бойынша жібереді.
26. Пікірталас жағдайларын шешуге қатысты сұратуларды Серіктес алдымен өз жағында қарастырады және оны шешу мүмкін болмаған жағдайда, Банктің Қолдау қызметіне api@tengribank.kz мекенжайы бойынша электрондық түрде осы Ережеге қосымшада белгіленген нысанда жібереді.
27. Серіктес оның немесе Банктің алаяқтық операциялардың жүргізілуі туралы күдіктері болса, мән-жайлар анықталғанға дейін операцияларды бұғаттауға міндетті.
28. Клиенттердің шоттары бойынша алаяқтық операциялар орын алған жағдайда, егер ол Серіктестің ақпараттық қауіпсіздік ережелерін/шараларын орындамау себебінен орын алса, оған шығынды өтеу үшін толық жауапкершілік жүктеледі.
29. Серіктеске техникалық себептер бойынша операцияларды жүргізу мүмкін болмағаны үшін (жұмыс істеуі Банкке байланысты емес байланыс желілерінің немесе коммуникациялық жабдықтардың ақаулығы) жауапкершілік жүктеледі.

4 тарау. ҚЫЗМЕТТЕРДІ ТОҚТАТА ТҰРУ ЖӘНЕ ТОҚТАТУ ТӘРТІБІ

30. Банк:

1) Серіктес Банк пен Серіктестің арасында жасалған Шартпен және осы Ережемен көзделген өз міндеттемелерін орындамаған жағдайда;

2) Серіктестің бастамасы бойынша, Банктің ішкі нормативтік құжаттарында белгіленген нысан бойынша ол Банкке өтініш берген күннен кейінгі жұмыс күнінен кешіктірмей;

3) Клиенттің бастамасы бойынша, Банктің ішкі нормативтік құжаттарында белгіленген нысан бойынша ол Банкке өтініш берген күннен кейінгі жұмыс күнінен кешіктірмей;

4) жүйедегі операциялар белгіленген талаптардың және Қазақстан Республикасының қолданыстағы заңнамасы, Шарт және осы Ереже бойынша талаптарды бұзумен жүргізілсе;

5) электрондық банктік қызметтердің ұсынылуын қамтамасыз ететін техникалық құралдардың ақаулығы болған кезде;

6) Банк Серіктестің өз авторландыру параметрлерін (пайдаланушы атауы, пароль немесе өзге параметрлер) басқа тұлғаларға жіберуін анықтаған кезден немесе егер Банктің пікірі бойынша осындай шара қажет болса өзге негіздемелер бойынша;

7) Банк қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимылға қатысты Қазақстан Республикасы заңнамасы талаптарының бұзылу фактілерін анықтаған кезде;

8) Серіктестің тіркеу куәлігін қайтарған немесе жойған кезде;

9) Қазақстан Республикасының қолданыстағы заңнамасымен, Шартпен және осы Ережемен көзделген өзге негіздер бойынша Серіктестің ақпараттық жүйелерінде электрондық банктік қызметтерді көрсетуді тоқтата тұруға немесе тоқтатуға құқылы.

31. Жоғарыда көрсетілген негіздер бойынша электрондық банктік қызметтерді орналастыруды тоқтата тұратын/тоқтатын жағдайда, Банк Серіктесті Шартта белгіленген тәртіппен және мерзімде хабардар етеді. Қызметтер себептерді жойған соң ғана қалпына келтіріледі.
32. Қызметтер тоқтатылатын жағдайда, Банк жұмыс күні ішінде Серіктестің Банктің электрондық жүйесіне қол жеткізуін бұғаттайды және осы факт туралы электрондық түрде Серіктестің ақпараттық жүйелері арқылы Банктің электрондық банктік қызметтерін пайдаланатын Банктің барлық Клиенттерін хабардар етеді.
33. Жоспарлы профилактикалық жұмыстардың аясында Серіктестің ақпараттық жүйелерінің жұмысын тоқтата тұрған жағдайда, бес күн бұрын Банк пен Банк клиенттерін жүргізілетін жұмыстардың уақыты және ұзақтығы туралы хабардар етуі тиіс.

5 тарау. ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТЫ ҚОРҒАУ ШАРАЛАРЫ

34. Банктің және Серіктестің электрондық банктік қызметтерді ұсынуы Клиенттің, Серіктестің және Банктің қауіпсіздік саясатына, Шарт пен осы Ережеге сәйкес жүргізіледі.
35. Қауіпсіздік шараларына жүйе бойынша электрондық банктік қызметтерді ұсыну кезіндегі ұйымдастырушылық шаралар және ақпараттық қауіпсіздікті қамтамасыз етудің бағдарламалық-техникалық қорғаныс құралдары енеді.
36. Банк және Серіктес Клиентке электрондық қызмет көрсету процесінде қолданатын қауіпсіздік шаралары:

    1) Серіктесті/Банктің және оның Клиенттердің жеке деректеріне қол жеткізу құқығын дәлме-дәл сәйкестендіруі;

    2) Клиентті және оның Серіктестің ақпараттық жүйелері арқылы тиісті электрондық банктік қызметтерді алу құқығын дәлме-дәл сәйкестендіруі;

    3) Клиентке соның негізінде электрондық банктік қызметтер ұсынылатын электрондық құжаттардағы бұрмалаушылықтардың және/немесе өзгерістердің болуын анықтауы;

    4) банктік құпияны құрайтын ақпаратты рұқсатсыз қол жеткізуден қорғауды қамтамасыз етуі және осы ақпараттың сақталуын қамтамасыз етуі тиіс.

37. Серіктес және Банк олардың негізінде Клиентке электрондық банктік қызметтер көрсетілген хабарламаларды жібергені және (немесе) алғаны туралы растауларды сақтауды қамтамасыз етеді.
38. Электрондық банктік қызметтерді ұсынудың түпнұсқалығы Серіктестің ішкі қауіпсіздік саясатымен және Банк пен Серіктес арасында жасалған Шартпен көзделген қауіпсіздік шараларын орындауы нәтижесінде анықталады.
39. Рұқсатсыз қол жеткізу немесе банктік құпияны құрайтын ақпаратқа осындай қол жеткізуге талпыну, оны рұқсатсыз өзгерту, рұқсатсыз төлем немесе ақша аударымын жүзеге асыру және Банк банктік электрондық қызмет көрсететін кезде туындайтын өзге рұқсатсыз іс-әрекеттер анықталған кезде, Банк ол туралы Серіктесті және керісінше Серіктес Банкті олар анықталғаннан кейінгі күнтізбелік күннен кешіктірмей электрондық байланыс арналары бойынша осындай хабарламаларды жіберу арқылы хабардар етеді.
40. Рұқсатсыз іс-әрекеттер туындаған жағдайда, Банк және/Серіктес дереу олардың салдарын жою және болашақта қайта пайда болуының алдын алу үшін барлық қажетті шараларды қабылдайды.
41. Банк немесе Серіктес рұқсатсыз төлемдер салдарынан қауіпсіздік деңгейін арттыру, алаяқтық және өзге арам ниетті іс-әрекеттердің және киберқауіпсіздік қауіптерінің алдын алу, құпия ақпараттың жария етілуіне және өзге құқыққа қарсы әрекеттерге жол бермеу мақсатында

электрондық банктік қызметтерді көрсету үшін қажетті қосымша талаптарды қарастыруы мүмкін.

42. Банк біржақты тәртіпте Клиент үшін жақсарту жағына қарай рұқсатсыз төлемдер, алаяқтық іс-әрекеттер, құпия ақпараттың жария етілуі немесе ақпараттық қауіпсіздіктің әлеуетті қауіптерін және тәуекелдерін анықтау және алдын алу аясындағы құқыққа қарсы өзге әрекеттер салдарынан қауіпсіздік рәсімдерін күшейту бойынша іс-шараларды жүзеге асыруға құқылы.
43. Серіктес заңсыз төлемнің жүргізілу фактісі анықталған жағдайда, серіктес ол туралы Банкті осындай төлем анықталған бір операциялық күннен кешіктірмей рұқсатсыз төлемді растайтын объективті айғақтарды қоса беру арқылы хабардар етеді.
44. Серіктестің ақпараттық жүйесіндегі құпия ақпаратқа қол жеткізу пайдаланушыларды ақпараттық жүйелерде аутентификациялаудың және авторландырудың ішкі ережелеріне сәйкес Клиентті сәйкестендіруден кейін ғана жүзеге асырылады.
45. Электрондық құжаттарды Банк олар жасалған, жіберілген немесе алынған нысанда олардың бүтіндігін және өзгермейтіндігін сақтай отырып, бес жыл мерзімге сақтайды және сақтау мақсатында электрондық құжатты басып шығаруды немесе оның мазмұнын қағаз тасымаладушыда өзгеше көрсетуді талап етпейді.
46. Серіктестің ақпараттық жүйелері арқылы электрондық банктік қызметтердің ақпараттық қауіпсіздігін қамтамасыз ету үшін екі тарап та келесі талаптарды орындайды:
    1) деректермен алмасу қорғалған арна бойынша жүргізіледі;
    2) әрбір хабарламаға оны жіберушінің ЭЦҚ қойылады;
    3) Серіктес банктің ақпараттық жүйелеріне HTTP/SSL хаттамасын пайдалану арқылы кіреді;
    4) Банк пен Серіктестің хабарламалармен алмасуға және ЭЦҚ орнатуға арналған тіркеу куәліктері Қазақстан Республикасы Ұлттық куәландырушы орталығы шығаруы тиіс;
    5) Серіктестің әр сұратуы JWS токені стандартына сәйкес келеді (қолтаңба алгоритмі RS512). Токен жіберуші жағында жинақталады және RS512 алгоритмін пайдалан отырып, RSA жабық кілтімен жасалған қолтаңбасы бар. Токен JWS әрбір сұрату үшін бірегей болып жасалады;
    6) Клиент құрылғысы мен Серіктестің ақпараттық жүйесі арасында деректермен алмасу HTTP/SSL хаттамасын пайдалану арқылы жүзеге асырылады.

6 тарау. ҚҰПИЯЛЫЛЫҚ

47. Банк және Серіктес Клиенттің құпия ақпаратын құрайтын ақпаратқа үшінші тұлғалардың рұқсатсыз қол жеткізуінің алдын алу үшін шаралар қабылдауға міндеттенеді. Осы сипаттағы кез келген ақпарат Қазақстан Республикасының қолданыстағы заңнамасында белгіленген тәртіппен ғана берілуі тиіс.
48. Есептік жазбалардың деректерін пайдалану қандайда бір құпия ақпаратты Серіктеске беруді немесе Банктің оны сақтауын білдірсе, Банк үшінші тұлғалардың осындай ақпаратқа оны Серіктеске бергенге дейін, сондай-ақ көрсетілген ақпарат сақталатын уақытта қол жеткізуінің алдын алу үшін барлық қажетті және Банкке байланысты ұйымдастырушылық және техникалық сипаттағы шараларды қабылдауға міндеттенеді.

7 бап. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

49. Осы Ережені лайықты түрде орындау үшін жауапкершілік Банктің жеке бөлімшелері басшыларына және Клиенттерге Серіктестің ақпараттық жүйелері арқылы электрондық банктік қызметтерді ұсыну процесіне тартылған Серіктестің лауазымды тұлғаларына жүктеледі. Осы Ережемен реттелмеген мәселелер Қазақстан Республикасы заңнамасының нормаларына және/немесе Банктің ішкі құжаттарына сәйкес шешіледі.
50. Осы Ережемен реттелмеген мәселелер Қазақстан Республикасы заңнамасының нормаларына және/немесе Банктің ішкі құжаттарына сәйкес шешіледі.

Правила
предоставления электронных банковских услуг через информационные системы третьих лиц

Настоящие Правила предоставления электронных банковских услуг через информационные системы третьих лиц (далее – Правила) регулируют отношения между АО "Tengri Bank" (далее – Банк) и третьим лицом (далее Партнер) в рамках дистанционного банковского обслуживания, а также общие требования, ограничения и процедуры предоставления электронных банковских услуг юридическим лицам и индивидуальным предпринимателям посредством информационных систем Партнера в соответствии с Договором. Правила разработаны в соответствии с законодательством Республики Казахстан и внутренними нормативными документами Банка (далее – внутренние документы).

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Правила являются неотъемлемой частью Договора аутсорсинга с Партнером, заключенного между Банком и Партнером. Заключая Договор аутсорсинга, Партнер присоединяется к настоящим Правилам и подтверждает:
   1) что получил, ознакомлен и, безусловно, согласен с настоящими Правилами;
   2) обязуется соблюдать и руководствоваться настоящими Правилами и требованиями действующего законодательства Республики Казахстан.
2. В настоящих Правилах используются определения, предусмотренные законодательством Республики Казахстан и внутренними документами, а также следующие понятия и условные обозначения:
   1) диспут, диспутная ситуация или спорная ситуация – ситуация по вопросам оказания электронной банковской услуги, в которой Клиент Банка не согласен с фактом или содержанием исполненного поручения Клиента, направляемый через официальные каналы;
   2) договор аутсорсинга (далее Договор) – договор между Партнером и Банком для предоставления электронных банковских услуг для Клиентов Банка через информационные системы Партнера;
   3) защищенный канал связи – канал связи, организованный между Банком и Партнером с применением технологий IPSec без возможности прослушивания или изменения данных, передаваемых между Банком и Партнером;
   4) конфиденциальная информация – банковская, коммерческая тайны и любая защищаемая законом информация, в том числе и персональные данные.
   5) Клиент – юридическое лицо/представительство/ индивидуальный предприниматель /частный нотариус/частный судебный исполнитель/ адвокат и профессиональный медиатор, которое/который на основании договорных отношений с Банком пользуется электронными банковскими услугами, с использованием системы и функций Партнера;
   6) открытый (публичный) ключ – последовательность электронных цифровых символов, сформированная удостоверяющим центром и доступная любому лицу и предназначенная для подтверждения подлинности Электронной цифровой подписи в Электронном документе;
   7) Партнер – юридическое лицо/индивидуальный предприниматель, осуществляющее (-ий) сотрудничество с Банком, с целью реализации дистанционных банковских услуг Клиентам Банка;

8) регистрационное свидетельство – документ в электронном виде, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным законодательством Республики Казахстан;

9) техническая документация – документация или любая техническая информация, необходимая для технического взаимодействия информационных систем Банка и Партнера. Документация размещается на интернет-ресурсе api.tengribank.kz;

10) удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

11) электронные банковские услуги – услуги, связанные с доступом Клиента к своему банковскому счету посредством системы для получения транзакционных (платежных) услуг и информационных банковских услуг в виде формирования Клиентом электронных документов.

12) электронная цифровая подпись (далее – ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания. ЭЦП позволяет установить автора электронного документа и/или средство аутентификации, с использованием которого осуществлена его передача и подтверждение, что документ не был изменен с момента его подписания.

3. Партнер оказывает Банку услуги по размещению в информационных системах Партнера электронных банковских услуг и обеспечивает доступ к ним Клиентов Банка.
4. Порядок предоставления электронных банковских услуг Клиентам через информационные системы Партнера регламентирован в Правилах предоставления электронных банковских услуг юридическим лицам и индивидуальным предпринимателям.
5. Перечень электронных банковских услуг, размещаемых в информационных системах Партнера:

   1) информационные банковские услуги (предоставление информации об остатках и движении по банковским счетам Клиента, просмотр истории платежей и переводов, информация о номере и валюте банковского счета, информации по депозитам, кредита, гарантиям и другим договорам Клиента, ставки вознаграждения, размера ежемесячного платежа, просмотр электронных копий договора, осуществленные платежи по депозитам, кредитам, гарантиям и т.д., предоставление информации об адресах отделений, курсах валют, продуктах и акциях Банка);

   2) транзакционные (платежные) банковские услуги (осуществление платежей и переводов с текущих счетов Клиентов, платежи в бюджет, платежи в пользу поставщиков услуг, безналичная конвертация);

6. Перечень электронных банковских услуг не является исчерпывающим и может дополняться Банком по своему усмотрению. Уведомление об изменении перечня производится путем размещения информации на интернет-ресурсе Банка (www.tengribank.kz).
7. Информационная система Партнера не относится к системно-значимой, значимой или иной платежной системе, а Партнер не является платежной организацией. При соответствии Партнера критериям, установленным законодательством для платежной организации, а его информационной системы – критериям системно-значимой, значимой или иной платежной системе условия Договора считаются нарушенными Партнером, Договор расторгается и Правила более не действуют в отношении Партнера с даты такого соответствия независимо от уведомления/не уведомления Партнером Банка и Клиента. Партнер возмещает нанесенный Банку и Клиенту ущерб в полном объеме и проводит необходимые мероприятия по возврату данных и закрытию доступа к системе Банка и данным Клиента в рамках своей Информационной системы.
8. В случае, если какое-либо положение Правил прекратит действовать по основаниям, предусмотренным законодательством, все остальные положения Правил продолжают действовать.
9. Подписанием Договора Партнер выражаю свое согласие на изменение и дополнение Банком Договора и/или Правил в одностороннем порядке, путем размещения новой редакции Договора

и/или Правил или внесенных изменений и дополнений в Договор и/или Правила на интернет-ресурсе Банка по адресу www.tengribank.kz.

Глава 2. ПОРЯДОК РАЗМЕЩЕНИЯ ЭЛЕКТРОННЫХ БАНКОВСКИХ УСЛУГ

10. Для начала предоставления электронных банковских услуг в информационных системах Партнеров должны быть выполнены следующие мероприятия:
    1) заключен Договор между Банком и Партнером;
    2) проведены технические работы по подключению информационных систем Партнера к системе дистанционного банковского обслуживания;
    3) в Банке открыт расчетный счет Партнера;
    4) предоставлен в Банк открытый ключ Партнера;
    5) организован защищенный канал связи между Банком и Партнером;
    6) согласован обеими сторонами документ Партнера "Правила информационной безопасности при работе в информационных системах с электронными банковскими услугами ";
    7) получено заключение подразделения информационной безопасности о соответствии схемы подключения требованиям ВНД в области информационной безопасности.

    Партнер гарантирует, что Партнером получено письменное согласие пользователей/ Клиентов на сбор, обработку и передачу Банку персональных данных (в том числе, трансграничную) Пользователя, при регистрации нового Пользователя в информационной системе Партнера для целей исполнения заключенных с Банком договоров.
11. При начале предоставления электронных банковских услуг Партнер может управлять через свои информационные системы только своими банковскими счетами и продуктами. Для предоставления электронных банковских услуг Клиентам Банка, Клиент должен предоставить в Банк заявление о согласии в получении электронных банковских услуг в информационной системе Партнера. Форма заявления и порядок его подачи регламентирован в Правилах предоставления электронных банковских услуг юридическим лицам и индивидуальным предпринимателям.
12. Для проведения технических работ по подключению Банк предоставляет доступ Партнеру к технической документации после подписания Договора.
13. Банк оставляет за собой право вносить изменения в техническую документацию и процедуры подключения по своему усмотрению, уведомив Партнера об этом не менее, чем за 15 (пятнадцать) календарных дней до внесения изменений.
14. Обмен информацией между Банком и Партнером осуществляется по защищенному каналу с подписанием каждого сообщения ЭЦП как со стороны Банка, так и Партнера.
15. Банк и Партнер обязаны проверять легитимность ЭЦП и открытых ключей с использованием удостоверяющего центра для каждого запроса и ответа и хранить журнал с результатами этих проверок не менее 5 лет.
16. Порядок подписания запросов Клиентов через информационные системы Партнера регламентирован в Порядке предоставления электронных банковских услуг.
17. Сообщение, полученное по защищенному каналу и имеющий корректное ЭЦП Партнера является равнозначным его бумажному носителю с печатью и подписью Партнера.
18. Сообщение, полученное от Партнера, считается полученным после прохождения всех проверок на корректность на стороне информационных систем Банка. Под корректностью подразумевается корректность ЭЦП и формата сообщения.

Глава 3. ПОРЯДОК РАЗРЕШЕНИЯ ДИСПУТНЫХ СИТУАЦИЙ И УВЕДОМЛЕНИЙ

19. Для эффективных коммуникаций в процессах сопровождения информационных систем и уведомлений о работе информационных систем Банка, Партнер сообщает в Банк контактные данные Службы поддержки Партнера.

20. Партнер обязан уведомлять Банк о всех случаях простоя своих информационных систем, через/в которых предоставляются электронные банковские услуги Банка в срок не позднее одного часа с момента выявления данного факта путем направления сообщения на адрес Службы поддержки Банка.
21. Партнер обязан каждый раз уведомлять в виде SMS Клиентов Банка, использующие информационные системы Партнера, о факте приостановления предоставления электронных банковских услуг Банка не позднее одного часа с момент выявления факта приостановления с предоставлением подтверждения Банку.
22. В случае возникновения диспутных ситуаций Партнер уведомляет Банк, с приобщением документов, подтверждающих обоснованность претензии (при их наличии) в течение 15 (пятнадцати) календарных дней с момента обнаружения Клиентом диспутной ситуации. Неполучение Банком такого заявления о спорной ситуации от Клиента в течение указанного срока считается подтверждением правильности совершения платежа или иной операции.
23. При проведении Банком проверки по диспутной ситуации, на основании полученного заявления, с целью снижения риска несанкционированных платежей, Банк, в интересах Клиента, вправе по своему усмотрению принять меры для предотвращения убытков и расходов Клиента, вплоть до приостановления предоставления электронных банковских услуг через информационные системы Партнера.
24. Более детально порядок разрешения диспутных ситуаций с платежами Клиентов приведен в Правилах предоставления электронных банковских услуг юридическим лицам и индивидуальным предпринимателям.
25. Все виды уведомлений Партнер направляет в Службу поддержки Банка в электронном виде по адресу api@tengribank.kz.
26. Запросы на разрешение диспутных ситуаций Партнер предварительно рассматривает на своей стороне и в случае невозможности его разрешения, направляет в Службу поддержки Банка в электронном виде по адресу api@tengribank.kz в форме, определенной в приложении к настоящим Правилам.
27. Партнер обязан блокировать операции при наличии у него или у Банка подозрений на мошеннические операции до выяснения обстоятельств;
28. В случае наступления мошеннической операции по счетам Клиентов Партнёр несет полную ответственность за возмещение ущерба, если она произошла по причине его неисполнения правил/мер информационной безопасности.
29. Партнер несет ответственность за невозможность проведения операции по техническим причинам (неисправность линий связи либо коммуникационного оборудования, работа которых не зависит от Банка).

Глава 4. ПОРЯДОК ПРИОСТАНОВЛЕНИЯ И ПРЕКРАЩЕНИЯ УСЛУГ

30. Банк имеет право приостановить или прекратить предоставление электронных банковских услуг в информационных системах Партнера в случае:

    1) неисполнения Партнером своих обязательств, предусмотренных Договором, заключенным между Банком и Партнером и настоящими Правилами;

    2) по инициативе Партнера, не позднее рабочего дня следующего за днем представления им заявления в Банк по форме, установленной внутренними нормативными документами Банка;

    3) по инициативе Клиента, не позднее рабочего дня следующего за днем представления им заявления в Банк по форме, установленной внутренними нормативными документами Банка;

    4) осуществления операций в системе с нарушением установленных требований и условий действующего законодательства Республики Казахстан, Договору и настоящими Правилами;

    5) при неисправности технических средств, обеспечивающих предоставление электронных банковских услуг;

6) при обнаружении Банком передачи информации Партнером собственных параметров авторизации (имя пользователя, пароль и иного параметра) другим лицам или по иным основаниям, в случае, если по мнению Банка, такая мера необходима;

7) при обнаружении Банком фактов нарушения требований законодательства Республики Казахстан в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

8) отзыв или аннулирование регистрационного свидетельства Партнера;

9) по иным основаниям, предусмотренным действующим законодательством Республики Казахстан, Договором и настоящими Правилами.

31. В случае приостановления/прекращения размещения электронных банковских услуг по указанным выше основаниям, Банк уведомляет Партнера в порядке и сроки, установленные Договором. Возобновление услуг возможно только после устранения причин.
32. В случае прекращения услуг, Банк в течении рабочего дня блокирует доступ Партнера к информационным системам Банка и уведомляет в электронном виде о данном факте всех Клиентов Банка, использующие электронных банковские услуги Банка через информационные системы Партнера.
33. В случае приостановления работы информационных систем Партнера в рамках плановых профилактических работ, за пять дней уведомить Банк и Клиентов Банка о времени и длительности проводимых работ.

Глава 5. МЕРЫ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

34. Предоставление Банком и Партнером электронных банковских услуг производится в соответствие с политикой безопасности Клиента, Партнера и Банка, Договором и настоящими Правилами.
35. Меры безопасности включают организационные меры и программно-технические средства защиты обеспечения информационной безопасности при предоставлении электронных банковских услуг по системе.
36. Меры безопасности, принимаемые Банком и Партнером в процессе электронного обслуживания Клиентов должны:

    1) достоверно идентифицировать Партнера/Банк и его право на доступ к персональным данным Клиента;

    2) достоверно идентифицировать Клиента и его право на получение соответствующих электронных банковских услуг через информационные системы Партнера;

    3) выявлять наличие искажений и/или изменений в электронных документах, на основании которых Клиенту предоставляются электронные банковские услуги;

    4) обеспечивать защиту от несанкционированного доступа к информации, составляющей банковскую тайну, и обеспечивать целостность данной информации.

37. Партнер и Банк обеспечивают хранение подтверждения об отправке и (или) получении сообщений, на основании которых Клиенту предоставлены электронные банковские услуги.
38. Подлинность предоставления электронных банковских услуг устанавливается в результате выполнения Партнером мер безопасности, предусмотренных его внутренней политикой безопасности и Договором, заключенным между Банком и Партнером.
39. При обнаружении несанкционированного доступа или попыток такого доступа к информации, составляющей банковскую тайну, ее несанкционированного изменения, осуществления несанкционированного платежа или перевода денег и иных несанкционированных действий, возникающих при оказании Банком электронных банковских услуг, Банк уведомляет об этом Партнера и наоборот, не позднее следующего календарного дня после их обнаружения путем направления таких уведомлений по электронным каналам связи.
40. В случае возникновения несанкционированных действий Банк и/или Партнер незамедлительно принимает все необходимые меры для устранения их последствий и предотвращения их появления в будущем.

41. Банком и Партнером могут быть предусмотрены дополнительные условия, необходимые для оказания электронных банковских услуг в целях повышения уровня безопасности от несанкционированных платежей, предотвращения мошеннических и иных злонамеренных действий, и угроз кибербезопасности, недопущения разглашения конфиденциальной информации, или иных противоправных действий.
42. Банк вправе в одностороннем порядке осуществлять мероприятия в сторону улучшения для Клиента, по усилению процедур безопасности от несанкционированных платежей, мошеннических действия, разглашения конфиденциальной информации, или иных противоправных действий в рамках выявления и предотвращения потенциальных угроз и рисков информационной безопасности.
43. В случае выявления Партнером факта осуществления несанкционированного платежа, Партнер уведомляет об этом Банк в срок не позднее одного операционного дня, в котором был обнаружен такой платеж, с приложением объективных свидетельств, подтверждающих несанкционированность платежа.
44. Доступ к конфиденциальной информации в информационной системе Партнера осуществляется только после идентификации Клиента, в соответствии с внутренними правилами аутентификации и авторизации пользователей в информационных системах.
45. Электронные документы хранятся сроком пять лет Банком в том формате, в котором они были сформированы, отправлены или получены с соблюдением их целостности и неизменности и не требуют распечатки или иного отображения содержания электронного документа на бумажном носителе с целью хранения.
46. Для обеспечения информационной безопасности электронных банковских услуг через информационные системы Партнера обеими сторонами соблюдаются следующие требования:

    1) обмен данными производится по защищенному каналу;

    2) каждое сообщение подписывается ЭЦП его отправителя;

    3) Партнер обращается к информационным системам банка с использованием протокола HTTP/SSL;

    4) регистрационные свидетельства Банка и Партнера для обмена сообщениями и установки ЭЦП должны быть выпущены Национальным Удостоверяющим центром Республики Казахстан;

    5) каждый запрос Партнера соответствует стандарту токена JWS (алгоритм подписи RS512). Токен собирается на стороне отправителя запроса и содержит подпись, созданную закрытым ключем RSA, используя алгоритм RS512. Для каждого запроса формируется уникальный токен JWS;

    6) обмен данных между устройством Клиента и информационной системой Партнера осуществляется с использованием протокола HTTP/SSL.

Глава 6. КОНФИДЕНЦИАЛЬНОСТЬ

47. Банк и Партнер обязуются принять меры для предотвращения несанкционированного доступа третьих лиц к информации, составляющей конфиденциальную информацию Клиента. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном действующим законодательством Республики Казахстан.
48. В случаях, когда использование данных учетных записей, предполагает передачу Партнеру либо хранение Банком какой-либо конфиденциальной информации, Банк обязуется принять все необходимые и зависящие от Банка меры организационного и технического характера для предотвращения доступа третьих лиц к такой информации до передачи ее Партнеру, а также во время хранения указанной информации.

Глава 7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

49. Ответственность за надлежащее исполнение данных Правил возлагается на руководителей самостоятельных подразделений Банка и должностных лиц Партнера, задействованных в процессе предоставления Клиентам электронных банковских услуг через информационные системы Партнера.
50. Вопросы, не урегулированные настоящими Правилами, подлежат разрешению в соответствии с нормами законодательства Республики Казахстан и/или внутренними документами Банка.

Приложение
к Правилам предоставления
электронных банковских услуг
через информационные системы
третьих лиц

Форма запроса на разрешение диспутной ситуации

№	Параметр	Значение
1	Дата и время выявления	
2	БИН клиента и наименование	
3	Краткое описание ситуации	
4	Какие работы были проведены на стороне Партнера	
5	Материалы анализа ситуации на стороне Партнера	
…	…	

Примечание: количество параметров не ограничено и может расширяться по усмотрению Партнера.