

«ForteBank» АҚ-та «Заңды тұлғаларға арналған интернет-банкинг/«Fortebusiness» интернет-банкингі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкингі» жүйесін пайдалану арқылы заңды тұлғаларға/жеке кәсіпкерлерге электронды банктік қызмет көрсетудің ережелері

КС- 02П-СУОД-027

Құжаттың атауына Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес өзгертулер енгізілген. 10.11.2021ж. №2021-489998 өтінім.

ӘЗІРЛЕУШІ:
ШОБ өнімдері мен сервисті дамыту бағыты

Нұр-Сұлтан қ.
2014 жыл

1. Жалпы ережелер

«ForteBank» АҚ-та «Занды тұлғаларға арналған интернет-банкінг/«Fortebusiness» интернет-банкінгі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкінгі» Жүйесін пайдалану арқылы заңды тұлғаларға/жеке кәсіпкерлерге электронды банктік қызмет көрсетудің осы Ережелері (бұдан әрі мәтін бойынша «Ережелер» деп аталады), Қазақстан Республикасының қолданыстағы заңнамаларына, «ForteBank» АҚ ішкі құжаттарына сәйкес жасалған және «Занды тұлғаларға арналған интернет-банкінг/«Fortebusiness» интернет-банкінгі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкінгі» Жүйесін пайдалану арқылы заңды тұлғаларға/жеке кәсіпкерлерге электронды банктік қызмет көрсетудің тәртібі мен талаптарын қарастырады.

«Занды тұлғаларға арналған интернет-банкінг/«Fortebusiness» интернет-банкінгі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкінгі» жүйелерінде бастапқы сәйкестендіру (тіркелу) кезінде Клиент (оның өкілі) Клиентке электронды банктік қызметтерді көрсету мақсатында оның дербес деректерін жинау мен өңдеуге өз келісімін береді.

Тармаққа Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес жаңа абзацпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

(Ереженің барлық мәтіні бойынша Басқарманың 09.07.2015ж. №39 шешіміне сәйкес өзгертулер енгізілген).

(Ереженің барлық мәтіні бойынша Басқарманың 25.06.2015 ж. №49 шешіміне сәйкес өзгертулер енгізілген).

(Ереженің барлық мәтіні бойынша Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес өзгертулер енгізілген (отырыстың №53 хаттамасы)).

(Ереженің барлық мәтіні бойынша Басқарманың 2019 жылғы 16 мамырдағы шешіміне сәйкес өзгертулер енгізілген (отырыстың №16 хаттамасы)).

(Ереженің барлық мәтіні бойынша Басқарманың 09.07.2021ж. №01/2021-78 шешіміне сәйкес өзгертулер енгізілген).

2. Ережеде қолданылатын терминдер мен анықтамалар

1) **Аутентификация** – Банк бекіткен Қауіпсіздік Процедураларын сәйкес электронды құжаттың құрастырылуының нақтылығы мен дұрыстығын растау;

2) **Банк** – "ForteBank" АҚ;

3) **Клиенттің Банктік шоты** – Клиенттің Банкте ашылған Ағымдағы және/немесе Жинақ шоты;

3-1) Биометрикалық сәйкестендіру – Клиенттің физиологиялық және биологиялық ерекшеліктерінің негізінде оның электронды банктік қызметтерді алу құқығын біржақты растау мақсатында Клиенттің жеке басын анықтау процедурасы;

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 3-1) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

4) **Шарт** – Банк пен Клиент арасында жасалған, өзгертулері мен толықтыруларымен, «Занды тұлғаларға арналған интернет-банкінг/«Fortebusiness» интернет-банкінгі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкінгі» Жүйесін пайдалану арқылы заңды тұлғаларға/жеке кәсіпкерлерге электронды банктік қызмет көрсету туралы Шарт, сонымен қатар Банктің www.forte.kz веб-сайтында және Клиент үшін қолжетімді кез келген тәсілмен жарияланған және Шартта келісілген Электронды банктік қызметтерді көрсетудің кез келген қосымша талаптары;

5) **Өтінім** – Электронды банктік қызметтерді көрсету туралы Шарттың №1 Қосымшасында/заңды тұлғаларға/«ForteBusiness»-ке арналған Интернет-банкінг жүйесінің Өтінішінің 4 Қосымшасында белгіленген үлгіге сәйкес ресімделген Заңды тұлғаларға арналған интернет-банкінг/«ForteBusiness» заңды тұлғаларға арналған мобильді интернет-банкінгіне қолжетімділік беруге өтінім. Клиенттің Өтініміне оның бірінші басшысы қол қояды және Клиенттің мөрімен (бар болса) бекітіледі немесе оған Уәкілетті өкіл қол қояды (және ол туралы тиісті Сенімхатта көрсетілген кезде мөрмен бекітіледі);

5-1) **Өтініш** – жүйені пайдалану арқылы клиенттердің банктік шоттары бойынша операцияларды жүргізудің Жалпы талаптарына қосылу туралы өтініші (Банктік қызмет көрсетудің жалпы талаптарына қосылу шарттарында клиенттердің жекелеген топтарына банктік қызметтердің түрін ұсыну тәртібі туралы Ереженің № 4 қосымшасы);

6) **Клиентті сәйкестендіру** – электронды банктік қызметтерді алу құқығын біржақты растау мақсатында Қолданушының/Клиенттің Уәкілетті өкілінің нақты өзі екендігін растау процедурасы;

7) **Клиент** – Шарт жасасқан заңды тұлға/жеке кәсіпкер;

8) **Байланыс деректері** – Клиенттің Электронды банктік қызметтерді алуға байланысты мәселелер бойынша Банкке хабарласатын Банктің/Банктің жауапты қызметкерлерінің байланыс телефондары мен мекенжайлары;

- 9) **Клиенттің логині** – Клиенттің бірегей логині (Қолданушының Логинімен бірге қолданылады), Жүйеде тіркелу үшін және әрі қарай Заңды тұлғаларға арналған интернет банкингі» арқылы Электронды банктік қызметтерге қолжетімділік алу үшін Банк барлық Қолданушыларға/Клиенттің Уәкілетті өкіліне береді;
- 10) **Қолданушының логині** – Жүйеде тіркелу үшін және әрі қарай Жүйеде Электронды банктік қызметтерге қолжетімділік алу мақсатында Банк беретін Жүйедегі Қолданушының/Клиенттің Уәкілетті өкілінің бірегей логині;
- 10-1) **«ForteBusiness» мобильді интернет-банкингі (Мобильді интернет- банкингі)** - Клиент - жеке кәсіпкердің¹ жеке кабинетте мобильді қосымша мен интернетке қолжетімділігі бар ұялы телефонда немесе басқа да құрылғы арқылы кіруге және банктік қызметтерді алуға арналған бағдарламалық қамсыздандыру;
Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 10-1) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.
- 10-2) **ҚР ҰКО** – Мемлекеттік және мемлекеттік емес ақпараттық жүйелерде электрондық құжаттарды қалыптастыру үшін жеке немесе заңды тұлғаларға электрондық цифрлық қолтаңба құралдарын және тіркеу куәліктерін беретін Қазақстан Республикасының Ұлттық куәландырушы орталығы;
Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 10-2) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.
- 11) **Жүйеге кіру ПИН-коды**- Жүйеге кіруге қажет жеке сәйкестендіру нөмірі. Банк «Заңды тұлғаларға арналған интернет банкингі» Жүйесінде әрбір Қолданушыға/Клиенттің уәкілетті өкіліне береді, әріптен, сандар мен символдар жиынтығынан тұратын, Жүйеге бірінші рет кірген соң ауыстырылуы тиіс, ашық түрде беріледі;
- 11-1) **Құпиясөз** – Электронды банктік қызметтерді алу үшін Клиенттің Банк Жүйесіне кіруге құқығын растауға арналған сандардың, әріптердің және басқа символдардың жиынтығы;
- 11-2) **Жалпы талаптар** – «Заңды тұлғаларға арналған интернет банкингі/«ForteBusiness» интернет банкингі/ «ForteBusiness» заңды тұлғаларға арналған мобильді интернет-банкингі» және «ForteBusiness» мобильді интернет-банкингі жүйесін пайдалану арқылы қашықтан қызмет көрсетуге қойылатын Жалпы талаптар
- 12) **ПИН** – құрылған кодты алу мақсатында Digipass Құрылғысын іске қосу үшін қажетті дербес сәйкестендіру коды. Банк «Заңды тұлғаларға арналған интернет банкингі/«ForteBusiness» интернет банкингі/ «ForteBusiness» заңды тұлғаларға арналған мобильді интернет-банкингі» Жүйесінде әрбір Қолданушыға/Клиенттің уәкілетті өкіліне береді;
- 12-1) **Жылдам кіру ПИН-коды**- құпия сандар жиынтығы, оның көмегімен Клиент Мобильді интернет-банкинге қолжетімділік ала алады;
Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 12-1) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.
- 13) **Клиенттің Жүйеге қосылуы** – Шарттың талаптарына және/немесе Клиенттің өтініміне сәйкес Жүйеде Қолданушының/Клиенттің Уәкілетті өкілін тіркеу;
- 14) **Филиалдың бөлімшесі** – Банк Филиалының қосымша жайы – бір облыс (республикалық маңызы бар қала, астана) аумағындағы бірнеше мекенжай бойынша орналасқан Бизнес сатылымдар басқармасы немесе Банктік қызмет көрсету орталығы;
- 15) **Қауіпсіздік процедурасы** – электрондық банктік қызметтерді алу құқығын белгілеу және берілетін және алынатын электрондық құжаттардың мазмұнындағы қателерді және/немесе өзгерістерді анықтау мақсатында электрондық құжаттарды жүйеге қосу, жасау, беру және алу кезінде Қолданушының/Клиенттің уәкілетті тұлғасын сәйкестендіруге арналған ұйымдастыру шараларының және ақпаратты қорғаудың бағдарламалық-техникалық құралдарының кешені;
- 16) **Клиенттің Қолданушысы (Қолданушы)** – Қазақстан Республикасының заңнамасында белгіленген тәртіппен Клиент өтінімінде көрсеткен, Шартқа сәйкес Жүйеге қол жеткізу құқығы және Клиенттің атынан Банкке нұсқауларға қол қою және жіберу құқықтарын қоспағанда, Клиенттің электрондық банк қызметтерін алуы үшін қажетті іс-әрекеттерді жүзеге асыру мүмкіндігі берілген тұлға;
- 17) **Клиенттің өкілі** – Клиенттің банктік шотын ашу кезінде Сенімхатқа сәйкес Клиенттің Банкке ұсынатын немесе Клиенттің атынан Банкке нұсқаулар беруге және қол қоюға, сонымен қатар Шарттың аясында қызметтерді алу мақсатында өзге де әрекеттерді орындауға құқылы, Клиент уәкілеттік берген, Клиенттің қолы мен мөр бедерінің үлгілері бар құжатта көрсетілген Клиенттің өкілі;
- 18) **Жұмыс күндері** – Қазақстан Республикасының заңнамаларына сәйкес демалыс немесе мереке болып табылмайтын күндер;

¹Мобильді интернет-банкинкте заңды тұлғаларға қызмет көрсету процесін техникалық жүзеге асыруды іске асырғанға дейін осы Жалпы талаптарда көрсетілген Сәйкестендіру, Аутентификациялау мен Мобильді интернет-банкингі пайдаланудың тәртібі тек қана Клиент-жеке кәсіпкерге қолданылады.

- 19) **Құрылған код** – бір реттік (біржолғы) код - бағдарламалық-аппараттық құралмен (Digipass құрылғысы) жасалатын және Клиентке электрондық банктік қызметтерге қолжетімділікті беру кезінде ұсынылатын бір реттік пайдалануға арналған электронды цифрлық символдардың бірегей бірізділігі;
- 20) **Жүйе** – «Заңды тұлғаларға арналған интернет банкинг/«ForteBusiness» интернет банкингі/«ForteBusiness» заңды тұлғаларға арналған мобильді интернет-банкінгі» бағдарламалық қамсыздандыру, ол арқылы Банк Клиентке электронды банктік қызметтерді ұсынады. Жүйеге қолжетімділік «Заңды тұлғаларға арналған интернет банкинг/«ForteBusiness» интернет банкингі» (<https://online.fortebank.com/>) / «ForteBusiness» заңды тұлғаларға арналған мобильді интернет-банкінгі» (<https://ibank.forte.kz/>), сонымен қатар мобильді қосымшасы орнатылған және интернеті бар ұялы телефон немесе басқа да құрылғы, IOS, Android арқылы іске асырылады;
- Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес мобильді интернет-банкінг анықтамасымен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.*
- 21) **Жинақ шоты** – Қазақстан Республикасының қолданыстағы заңнамасының талаптарына сәйкес банктік салым шартында көзделген операцияларды орындау үшін Банктік салым шарты негізінде Банктің Клиентке ашатын банктік шот;
- 22) **Ағымдағы шот** – Қазақстан Республикасының қолданыстағы заңнамасының талаптарына сәйкес банктік шот шартында көзделген операцияларды орындау үшін банктік шот шарты негізінде Банк Клиентке ашатын банктік шот;
- 23) **ForteX** – Банктің электронды өтінімдер арқылы электронды банктік қызметтерді көрсетуіне арналған «Интернет-банкінг және «ForteBusiness» /Заңды тұлғаларға арналған интернет-банкінгінің бағдарламалық қамсыздандыруының модулі/бөлімі;
- 24) **Digipass құрылғысы** – Шарттың және осы Ережесінің талаптарына сәйкес Банктің Клиентке берген құрылған/жасалған коды. Бұл ретте Digipass құрылғысын іске қосу үшін ПИН қолданылады. Digipass құрылғысы осы Ереженің №1 Қосымшасында қарастырылған;
- 25) **Уәкілетті орган** – Қазақстан Республикасының заңнамасына сәйкес Қазақстан Республикасының мемлекеттік органдары немесе банк шоттарындағы ақшаға тыйым салуға және/немесе банк шоттары бойынша шығыс операцияларын тоқтата тұруға уәкілеттік берілген өзге де лауазымды адамдар;
- 26) **Клиенттің Уәкілетті өкілі** – Клиент атынан банкке электрондық құжаттарға қол қоюға және жіберуге құқылы клиенттің банктік шотын ашу/ForteX модулінде операциялар жүргізу кезінде клиент Қазақстан Республикасының заңнамасына сәйкес Банкке ұсынатын Клиенттің қол қою үлгілері және мөр бедерлері бар құжатта көрсетілген Қолданушы/Клиенттің өкілі;
- 27) **Филиал** – Клиент барып банктік операцияларды іске асырған Банктің оқшауланған бөлімшесі;
- 28) **Электронды банктік қызметтер (Қызметтер)** – Банк Клиентке Қазақстан Республикасының нормативтік құқықтық актілерінде, Шартта және осы Ережеде белгіленген тәртіппен және шарттарда Жүйе арқылы қашықтықтан ұсынатын банктік қызметтер;
- 28-1) **Электронды құжат** – аппарат электрондық-цифрлық нысанда ұсынылған және сәйкестендіру құралдарымен куәландырылған, жөнелтуші жасаған және Қазақстан Республикасының заңнамасында көзделген тәртіппен жасалғаннан кейін оған енгізілген бұрмалауларды және (немесе) өзгерістерді қамтымайтын құжат;
- 29) **Электронды өтінім** - ForteX модулінде «Заңды тұлғаларға арналған Интернет-банкінг"/«ForteBusiness» жүйесі арқылы айырбастау жүргізу үшін Клиент жіберетін өтінім. Клиенттің электрондық өтініміне Клиенттің Уәкілетті өкілі қол қояды;
- 29-1) **СМС – код** – заңды тұлғаларға арналған Интернет - банкінгте /«ForteBusiness» заңды тұлғаларға арналған Интернет-банкінгте пайдаланылатын Қолданушының сұратуы бойынша Банктің бағдарламалық-техникалық құралдарымен жасалатын, Клиенттің уәкілетті өкілінің өтінімде көрсетілген ұялы телефон нөміріне SMS-хабарлама арқылы жіберілген және Қолданушыға электронды банктік қызметтерге қол жеткізуді ұсыну кезінде бір реттік пайдалануға арналған бірегей жүйелі электрондық цифрлық символдардан тұратын бір реттік (біржолғы) код;
- 29-2) **Электронды-цифрлы қолтаңба (ЭЦҚ)** – ЭЦҚ арқылы құрастырылған және электронды құжаттың растығын, оның сәйкестендіру құралы болып табылатын мазмұнының тиесілілігі мен өзгермейтінділігін растайтын электронды цифрлы символдардың жиыны;

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 29-2) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

- 29-3) **FaceID**- Клиенттің бет-әлпетінің көлемді - кеңістіктік формасының сканері, оның көмегімен құрылғының құлпын қауіпсіз ашуға, Мобильді интернет-банкінгке кіруге болады;

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 29-3) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

- 29-4) **TouchID**- Клиенттің саусақ ізі арқылы сәйкестендіретін жүйе, оның көмегімен құрылғының құлпын қауіпсіз ашуға, Мобильді интернет-банкінгке кіруге болады;

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 29-4) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

29-5) SMS-верификация- Клиентке Мобильді интернет – банкинкте сәйкестендіру немесе аутентификациялау кезінде енгізілетін ұялы телефон нөміріне СМС-коды бар SMS-хабарлама жіберу арқылы динамикалық сәйкестендіру процесі.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 29-5) тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

(Ереженің 2 бөлімі Басқарманың 2017 жылғы 05 шілдедегі шешіміне сәйкес жаңа редакцияда мазмұндалған (отырыстың №53 хаттамасы).

(Ереженің 2 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

3. Электронды банктік қызметтер тізімі

Банк Клиентке Шарт пен осы Ережеде бекітілген тәртіп пен талаптарда Электронды банктік қызметтерді көрсетеді.

1. Электронды банктік қызметтерге мыналар кіреді:

1.1. Ақпараттық-банктік қызметтер:

- 1.1.1. Өтінімге сәйкес Жүйеге қосылған Клиенттің Банктік шоттарына қолжетімділік беру;
- 1.1.2. Клиенттің Банктік шоттары бойынша қалдық және(немесе) қозғалыстар жайлы, Клиенттің шоттары бойынша төлемдер және(немесе) аударымдар туралы ақпарат беру;
- 1.1.3. төлемді алушылардың (бенефициарлардың) тізімін, оның ішінде қажетті өзгерістерді енгізуді қосу;
- 1.1.4. төлемдердің және (немесе) аударымдардың тарихын қарау;
- 1.1.5. болашақта бір типтес төлемдерді және (немесе) аударымдарға арналған шаблондарды құру;
- 1.1.6. электронды хабарламалар арқылы қауіпсіз байланыс арналары арқылы Банкпен байланысу (Банктің жауап беру мерзімі мен тәртібі «ForteBank» АҚ банктік операцияларын жүргізудің жалпы талаптары туралы Ережеде нақтыланған);
- 1.1.7. банктік шот ашу².

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 1.1.7 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

1.2. Төлем қызметтері:

- 1.2.1. Клиенттің Банктік шоттарындағы теңгедегі және шетел валютасында төлемдерді және(немесе) ақшалай аударымдарды жүргізуді іске асыру;
- 1.2.2. Шетел валютасын сату мен сатып алуды іске асыру, айырбастау операцияларын жүргізу;
- 1.2.3. Клиенттің Банктік шоттары бойынша үнемі қолданыстағы нұсқаулықтар (электронды құжаттар) құрастыру, өзгерту немесе жою;
- 1.2.4. болашақ күнге Клиенттің Банктік шоттары бойынша төлемдер мен аударымдарды құрастыру бойынша электронды құжаттарды жасау;
- 1.2.5. төлем карточкаларын шығару/қызмет көрсету³.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 1.2.5 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

1.3. Басқа қызметтер:

- 1.3.1. "ForteBusiness" жүйесі арқылы банктік қызметтерді алу үшін өтінімдер беру .

2. Бұл толық тізім болып табылмайды және Жүйенің дамуына байланысты Банк бір жақты тәртіпте өзгертуі/толықтыруы мүмкін, ол жайлы Банк өзінің Клиенттерін Банктің ресми www.forte.kz сайтында тиісті ақпаратты орналастыру арқылы құлақтандырады.

(Ереженің 3 бөліміне Басқарманың 2017 жылғы 05 шілдедегі шешіміне сәйкес өзгерістер енгізілген (отырыстың №53 хаттамасы).

(Ереженің 3 бөліміне Басқарманың 2019 жылғы 16 мамырдағы шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы).

(Ереженің 3 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

4. Электронды банктік қызметтерді көрсету тәртібі, тәсілі мен шарттары

² тек мобильді интернет-банкинкте ғана қолжетімді

³ тек мобильді интернет-банкинкте ғана қолжетімді

3. Клиентке электронды банктік қызметтерге қолжетімділік Интернет желісіне қосылған кез келген құрылғыдан Интернет арқылы қорғалған арналар бойынша қашықтан ұсынылады.

4. Клиентке Электронды банктік қызметтерге қолжетімділік Жүйеде Қолданушының/Клиенттің Уәкілетті өкілінің біреуінің тіркеуден өткен соң беріледі. Бұл ретте төлем қызметтерін жүргізу тек төлем қызметтерін алу үшін Банкке Клиенттің электронды құжатты ұсынуға қажетті және жеткілікті құқығы бар Уәкілетті өкілі тіркелген жағдайда ғана іске асырылады.

5. Ақпараттық-банктік қызметтерді көрсету Клиент сәтті сәйкестендіру мен Аутентификациядан өткен жағдайда жүзеге асырылады.

6. Төлем қызметтерін көрсету Клиенттің Қауіпсіздік процедураларына сәйкес сәйкестендіру мен Аутентификациядан сәтті өткен жағдайда жүргізіледі. Бұл ретте төлем қызметтерін ұсыну клиенттің төлем қызметтерін алу үшін Банкке клиенттің электрондық құжаттарын ұсынудың қажетті және жеткілікті құқықтары бар уәкілетті тұлғалары тіркелген жағдайда ғана жүзеге асырылады. Аутентификация кезінде Digipass құрылғысы арқылы клиентті динамикалық сәйкестендіру қолданылады.

(Ереженің 4 бөліміне Операциялық комитеттің 2019 жылғы 16 мамырдағы шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы)).

«Занды тұлғаларға арналған интернет-банкінг» Жүйесінде Қолданушының/Клиенттің Уәкілетті өкілінің тіркелу тәртібі мен шарттары.

6.1. Қолданушының/Клиенттің уәкілетті өкілінің «Занды тұлғаларға арналған Интернет-банкінг» жүйесінде тіркелуі Интернет желісіне қолжетімділігі бар кез келген компьютерден Интернет арқылы жүзеге асырылады. Бұл ретте Қолданушы/Уәкілетті өлке қауіпсіздік процедураларын сақтауға міндетті.

6.2. Қолданушының/Клиенттің уәкілетті өкілінің «Занды тұлғаларға арналған Интернет-банкінг» жүйесінде тіркелуі үшін Қолданушыға/Клиенттің уәкілетті өкіліне Банктен Клиенттің Логинін, Қолданушының логинін, жүйеге кіруге арналған ПИНді (бастапқы), ПИНді (бастапқы), Digipass Құрылғысын алу қажет.

6.3. Клиенттің Логинін, Қолданушының Логинін Банк Клиенттің қатысуынсыз өз бетінше құрастырады.

6.4. Клиенттің Логині, Қолданушының логині, жүйеге кіруге арналған ПИН (бастапқы), ПИН (бастапқы), Digipass Құрылғысы Қолданушыға/Клиенттің уәкілетті өкіліне Қолданушыға/Клиенттің уәкілетті өкіліне шарт жасалған күннен бастап 10 (он) жұмыс күні ішінде Қолданушы/Клиенттің өкілі Банкке өзі келген кезде және Қолданушы/Клиенттің өкілі шартта белгіленген нысан бойынша қабылдау-тапсыру актісіне қол қойған жағдайда беріледі.

6.5. «Занды тұлғаларға арналған Интернет-банкінг» Жүйесінде Қолданушының/Клиенттің уәкілетті өкілін тіркеу «Занды тұлғаларға арналған Интернет-банкінг» жүйесінің тиісті веб-мекенжайы арқылы Клиенттің Қолданушысы/Уәкілетті өкілі Жүйеге кіру үшін Клиенттің Логинін, Қолданушының логинін, ПИН және Құрылған кодты енгізу арқылы жүзеге асырылады.

6.6. Қауіпсіздік процедураларын сақтау мақсатында, Digipass құрылғысын алу кезінде Қолданушы/Уәкілетті өкіл қауіпсіздік процедураларының талаптарына, осы Ереженің шарттарына және Ереженің №1 Қосымшасына сәйкес Банктен дербес ПИН-ге алынған бастапқы ПИН-ді ауыстыруға міндетті.

6.7. Жүйеге кіру үшін ПИН (бастапқы) Қолданушыға/Клиенттің уәкілетті өкіліне қауіпсіздік процедураларын сақтау мақсатында «Занды тұлғаларға арналған Интернет-банкінг» жүйесіне алғаш рет кірген кезде ашық түрде беріледі, Жүйеге кіру үшін оның дербес ПИН-ге ауысуы талап етіледі.

6.8. Қолданушы Логині және/немесе жүйеге кіру үшін ПИН және/немесе ПИН және/немесе Digipass құрылғысы жоғалған және/немесе Digipass құрылғысы бұзылған жағдайда, Қолданушы/Клиенттің уәкілетті өкілі Клиенттің тиісті түрде ресімделген хатының негізінде Қолданушының жаңа логинін және/немесе жүйеге кіру үшін ПИН (бастапқы) және/немесе ПИН (бастапқы) және/немесе Digipass құрылғысын алуға құқылы. Жүйеге(бастапқы) және/немесе ПИН (бастапқы) және/немесе Digipass құрылғысына кіру үшін Қолданушының жаңа логинін және/немесе ПИН (бастапқы) және/немесе ПИН (бастапқы) алу Клиенттің/Қолданушының/Клиент өкілінің Банкке өзі келуі кезінде және Клиент/Қолданушы/ Клиент өкілі Шартта белгіленген нысан бойынша қабылдау-тапсыру актісіне қол қойған жағдайда жүзеге асырылады.

6.9. Клиенттің банктік шоттарын Электрондық банктік қызметтерді алу үшін «Занды тұлғаларға арналған Интернет-банкінг» жүйесіне қосу және оларды «Занды тұлғаларға арналған Интернет-банкінг» жүйесінен алып тастау Шарт талаптарына сәйкес іске асырылады.

6.10. Клиентті «Занды тұлғаларға арналған Интернет-банкінг» Жүйесіне қосу Шартының талаптарына сәйкес жүргізіледі.

7-1. Қолданушының/Клиенттің Уәкілетті өкілін «ForteBusiness» Жүйесінде тіркеу тәртібі мен шарттары:

7-1.1. Қолданушыны/Клиенттің Уәкілетті өкілін Жүйеде тіркеу Интернет желісіне қолжетімділігі бар кез келген құрылғыдан Интернет арқылы жүзеге асырылады. Бұл ретте Қолданушы/Уәкілетті өкіл Қауіпсіздік процедураларын сақтауға міндетті.

7-1.2. Қолданушыны/Клиенттің Уәкілетті өкілін Жүйеде тіркеу үшін Қолданушыға/Клиенттің Уәкілетті өкіліне Банктен Қолданушының логинін, Құпиясөзді, ПИНді (бастапқы), Digipass құрылғысын алу қажет.

7-1.3. Клиенттің Логині, Қолданушының логині, жүйеге кіруге арналған ПИН (бастапқы), ПИН (бастапқы), Digipass Құрылғысы Қолданушыға/Клиенттің уәкілетті өкіліне Қолданушыға/Клиенттің уәкілетті өкіліне шарт жасалған күннен бастап 10 (он) жұмыс күні ішінде Қолданушы/Клиенттің өкілі Банкке өзі келген кезде және Қолданушы/Клиенттің өкілі шартта белгіленген нысан бойынша қабылдау-тапсыру актісіне қол қойған жағдайда беріледі.

7-1.4. Жүйеде Қолданушыны/Клиенттің уәкілетті өкілін тіркеу Жүйенің тиісті веб-мекенжайы арқылы Клиенттің Қолданушысы/Уәкілетті өкілі Жүйеге кіру үшін Клиенттің Логинін, Қолданушының логинін, ПИН және Құрылған кодты енгізу жолымен жүзеге асырылады.

7-1.5. Қауіпсіздік процедураларын сақтау мақсатында, Digipass құрылғысын алу кезінде Қолданушы/Уәкілетті өкіл қауіпсіздік процедураларының талаптарына, осы Ереженің шарттарына және Ереженің №1 Қосымшасына сәйкес Банктен дербес ПИН-ге алынған бастапқы ПИН-ді ауыстыруға міндетті.

7-1.7. ПИН және/немесе Digipass құрылғысы және/немесе Digipass құрылғысы бұзылған жағдайда, Қолданушы/Клиенттің уәкілетті өкілі Клиенттің тиісті түрде ресімделген хатының негізінде ПИН және / немесе Digipass құрылғысын алуға құқылы. Жаңа ПИН алу және/немесе Digipass құрылғысы Клиенттің/Қолданушының/Клиент өкілінің банкке жеке келуімен және Клиент/Қолданушы/Клиент өкілі нысан бойынша қабылдау-тапсыру актісіне қол қойған жағдайда жүзеге асырылады.

Құпиясөзді Жүйеге қатарынан 3 (үш) реттен көп қате көрсеткен жағдайда «ForteBusiness» жүйесі Жүйеге кіру мүмкіндігін бұғаттайды. Клиентке «ForteBusiness» Жүйесіне қолжетімділік Құпиясөзді арылған және/немесе қалпына келтірген жағдайда берілуі мүмкін. Құпиясөзді ауыстыру үшін Клиент басты терезедегі «Құпиясөзді қалпына келтіру» батырмасын басуы қажет, бұдан кейін Банк Клиенттің ұялы телефонына СМС-код жібереді. Егер Клиент «ForteBusiness» Жүйесіне кіру Құпиясөзін ұмытқан болса, онда ол жоғарыда айтылған әрекеттерді іске асыруға құқылы. Банк құпиясөзді қалпына келтіруді Клиенттің/Қолданушының/Клиенттің Өкілінің өтініші бойынша бір реттік Құпиясөзді құру арқылы іске асыра алады.

7-1.8. Электронды банктік қызметтерді алу және оларды Жүйеден алып тастау үшін Клиенттің Банктік шоттарын Жүйеге қосу Клиенттің қосу туралы өтінішінің талаптарына сәйкес іске асырылады.

7-1.9. Клиентті Жүйеге қосу жүйені пайдалану арқылы клиенттердің банктік шоттары бойынша операцияларды жүргізудің Жалпы талаптары туралы өтініштің талаптарына сәйкес жүргізіледі.

7-2. Мобильді интернет-банкінгте Клиентті Сәйкестендіру тәртібі мен талаптары:

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.1 Мобильді интернет-банкінгте Клиентті Бастапқы Сәйкестендіру (тіркеу) Банктің қосымшасын оқи алатын және Интернетке қолжетімділігі бар ұялы телефон немесе басқа да құрылғы арқылы іске асырылады. Бұл ретте Клиент Қауіпсіздік процедураларын сақтауға міндетті.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.1 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.2 Мобильді интернет-банкінгте Клиентті Бастапқы Сәйкестендіру (тіркеу) екі тәсілдің бірімен жүзеге асырылады:

1. SMS-тексеру мен биометрикалық сәйкестендіруді жүргізу арқылы (сонымен қатар Клиент жеке сәйкестендіру нөмірін енгізеді);

2. ЭЦҚ мен SMS-тексеру арқылы (жеке сәйкестендіру нөмірі ЭЦҚ-дан алынған мәліметтер негізінде автоматты түрде енгізіледі).

Мобильді интернет-банкінгте Бастапқы Сәйкестендіру (тіркеу) кезінде Клиент Құпиясөзді орнату қажет, логин ретінде оның ұялы телефоны жүреді. Сонымен қатар Клиентке FaceID, TouchID мен жылдам кіру ПИН-кодды орнату ұсынылады.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.2 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.3 Мобильді интернет-банкінгке келесі кіру Клиенттің логин мен құпиясөзді енгізуі, сонымен қатар SMS-тексеруді қолдану арқылы, немесе FaceID/TouchID/жылдам кіру ПИН-кодды қолдану арқылы іске асырылады. FaceID/TouchID/жылдам кіру ПИН-код орнату кезінде Мобильді интернет-банкінг Клиенттің енгізген логині мен Құпиясөзін есіне сақтайды және Мобильді интернет-банкінгке әрбір кірген кезде FaceID/TouchID /жылдам кіру ПИН-код ын қолданған кезде автоматты түрде Құпиясөзді енгізеді. Клиент Жалпы талаптарға қосылған кезде Мобильді интернет-банкінгке кірудің көрсетілген тәсілімен келіседі.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.3 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.4 Клиент Құпиясөз бен жылдам кіру ПИН-кодын үшінші тұлғаларға айтпауы/бермеуі және сақталуын қорғауы тиіс, сонымен қатар Мобильді интернет-банкінгке рұқсатсыз қолжетімділікті болдырмаудың алдын алу мақсатында ұялы/басқа да құрылғыға үшінші тұлғалардың FaceID/TouchID орнатпауы тиіс.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.4 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.5 Мобильді интернет-банкінгке кіру үшін Клиент қолданатын ұялы телефон нөмірін өзгертуді Клиент өз бетінше Мобильді интернет-банкінгте Жалпы талаптардың №2 Қосымшасына қол қою арқылы іске асырады.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.5 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.6 Құпиясөзді қатарынан 3 (үш) реттен көп қате көрсеткен жағдайда Жүйе Мобильді интернет-банкінгке кіру мүмкіндігін бұғаттайды. Клиент Жүйеге қолжетімділікті Құпиясөзді арылтқан және қалпына келтірген жағдайда берілуі мүмкін. Құпиясөзді ауыстыру үшін Клиент басты терезедегі батырманы басуы қажет.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.6 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

7-2.7 Жүйеде электронды банктік қызметтерді ұсыну Өтініш беру арқылы Жалпы талаптарға қосылу негізінде жүргізіледі.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 7-2.7 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

(Ереженің 4 бөліміне Операциялық комитеттің 2019 жылғы 16 мамырдағы шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы).

(Ереженің 4 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

7. Ақпараттық-банктік қызметтерді беру тәртібі мен шарттары:

7.1. Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес 8.1. тармақ алынып тасталды (отырыстың №53 хаттамасы).

8.2. «Заңды тұлғаларға арналған интернет-банкінг» Жүйесінде Қолданушыны/Клиенттің Уәкілетті өкілін Сәйкестендіру және Аутентификациялау тәртібі.

8.2.1. Жүйеде Клиентті Сәйкестендіру мен Аутентификациялау Қолданушының/Клиенттің Уәкілетті өкілінің Жүйенің тиісті электронды терезесінде тиісті түрде Клиенттің Логинін, Қолданушының логинін, жылдам кіруге арналған ПИНді және Құрылған кодты енгізу арқылы іске асырады.

8.2.2. Қолданушы/Клиенттің Уәкілетті өкілі Клиенттің Логинін, Қолданушының логинін, жылдам кіруге арналған ПИНді және Құрылған кодты дұрыс көрсетсе, Жүйеде Клиенттің сәйкестендірілуі тиісті түрде орындалған болып саналады және Қолданушы/Клиенттің Уәкілетті өкілі Электронды банктік қызметтерге қолжетімділік алады.

8.3. «ForteBusiness» Жүйесінде Қолданушыны/Клиенттің Уәкілетті өкілін Сәйкестендіру және Аутентификациялау тәртібі.

8.3.1. Жүйеде Клиентті Сәйкестендіру мен Аутентификациялау Қолданушының/Клиенттің Уәкілетті өкілінің «ForteBusiness» Жүйесінің тиісті электронды терезесінде тиісті түрде Клиенттің Логинін, Қолданушының логинін, жылдам кіруге арналған ПИНді және Құрылған кодты енгізу арқылы іске асырады.

8.3.2. Аутентификациялау Қолданушының/Клиенттің Уәкілетті өкілінің Құрылған кодты қолдану арқылы Электронды құжаттарға қол қоюы арқылы жүргізіледі.

8.4. Қолжетімділік алған соң Қолданушы/Клиенттің Уәкілетті өкілі Жүйе арқылы Ақпараттық-банктік қызметтерді өз бетінше алуға құқылы:

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 8.5 тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

8.5.1. Аутентификациялау Клиенттің Электронды құжаттарға SMS-тексеру немесе ЭЦҚ пайдалану арқылы қол қоюмен іске асырылады.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 8.5.1. тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

8.5.2. Мобильді интернет-банкінге қолжетімділік алған соң Клиент Жүйе арқылы Ақпараттық-банктік қызметтерді өз бетінше алуға құқылы.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 8.5.2. тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

8.5.3. Мобильді интернет-банкінгің интерфейсі Клиенттің таңдауы бойынша орыс және қазақ тілдерінде жұмыс жасайды.

Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес 8.5.3. тармақпен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

(Ереженің 4 бөліміне Операциялық комитеттің 2019 жылғы 16 мамырдағы шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы).

(Ереженің 4 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

8. Төлем қызметтерін көрсетудің тәртібі мен шарттары:

8.1. Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес 9.1. тармақ алынып тасталды (отырыстың №53 хаттамасы).

8.2. Клиенттің дәл өзі екендігін анықтау мақсатында Қолданушы/Уәкілетті өкіл жүйеге кіруге арналған ПИНді/Құпиясөзді және Digipass құрылғысында жасалған Құрылған кодты енгізу арқылы Клиентті сәйкестендіру жүргізіледі. Сәйкестендіру оның электронды банктік қызметтерді алу құқығын нақты растау мақсатында іске асырылады.

8.3. Тиісті түрде Аутентификацияланған жағдайда Клиентке төлем қызметтері ұсынылады.

8.4. Төлем қызметтері Банк акцепттеген жағдайда Клиенттің электронды құжаттарының негізінде ұсынылады.

8.5. Төлем қызметтерін алу барысында Клиент Жүйеде автоматты түрде және Қазақстан Республикасының қолданыстағы заңнамасына сәйкес құрылған электронды құжаттардың үлгілерін қолданады.

8.6. Электронды құжаттарды Қолданушы ресімдейді және Клиенттің Уәкілетті өкілі қол қояды. Клиенттің төлем құжаттарына Клиенттің қол қою құқығына ие бірнеше Уәкілетті өкілдері қол қоюы тиіс болған жағдайда, Клиенттің электронды құжаттары Клиенттің тиісті тапсырмасына және Қазақстан Республикасының заңнамаларына сәйкес электронды құжаттарға Уәкілетті өкілдері қол қойған соң ғана Банкке тиісті түрде ұсынылған болып саналады.

8.7. Жүйе арқылы шетел валютасындағы төлемдер және(немесе) аударымдар Қазақстан Республикасының валюталық реттеу және валюталық қадағалау туралы заңнамасын сақтау арқылы іске асырылады.

8.7.1. Электрондық банктік қызметтерді шетел валютасында көрсету кезінде қолданылатын валюта айырбастау бағамын Банк операция жүргізу сәтінде айқындайды.

8.8. Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес 9.8. тармақ алынып тасталды (отырыстың №53 хаттамасы).

8.9. Қазақстан Республикасының қолданыстағы заңнамасында көзделген жағдайларда, сондай-ақ Шартта және банк шотының тиісті шарттарында көзделген өзге де жағдайларда Банк электрондық құжаттарды акцептеуден бас тарта алады.

(Ереженің 4 бөлімінің 9 тармағына Басқарманың 2017 жылғы 05 шілдедегі шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы).

4-1. ForteX модулінде айырбастау жүргізу

9.9-1. ForteX модулі арқылы айырбастауды жүргізу Қазақстан Республикасының валюталық реттеу және валюталық қадағалау туралы заңнамасын сақтау арқылы іске асырылады.

9.9-2. ForteX-те айырбастау кезінде қолданылатын валюта айырбастау бағамын Банк операция жүргізу сәтінде айқындайды және Клиент бағамды растаған сәттен бастап шектеулі уақыт ішінде әрекет етеді.

9.9-3. ForteX модулінде шектеулі уақыт ішінде айырбастауға акцепт пен электронды Өтінімге қол қою ForteX модулінде өтінімге қол қою Клиенттің барлық Уәкілетті өкілдері жүзеге асырады.

9.9-4. ForteX модулінде айырбастауға арналған электронды Өтінімді Банктің орындауы автоматты режимде іске асады. Электронды қол қою өтінімді ресімдеу кезінде қате мәліметтер енгізілген болса осы электронды өтінім орындалуға жатпайды.

9.9-5. ForteX модулінде клиенттің осындай уәкілетті өкіліне (қажет болған жағдайда) тиісті сенімхатпен бірге ForteX модулінде операция жүргізілгенге дейін Банкке ұсынылатын қол қою үлгілері және мөр бедері (бар болса)бар жеке құжатта көрсетілген Клиенттің уәкілетті тұлғасының айырбастауын жүргізуге рұқсат етіледі;

9.9-6. ForteX модулінде операцияларды жүргізу кезінде, клиент:

- 1) Банктің ForteX модулі арқылы құжаттарды алуы ҚР заңнамасының талаптарына сәйкес ресімделген және клиент өз қолымен қол қойған қағаз нұсқадағы құжаттарды алуға заңды түрде баламалы екенін мойындайды;
- 2) орындау үшін ForteX модулі арқылы Банкке жіберілген құжаттардың мазмұны үшін және осындай құжаттар туындататын құқықтық салдарлар үшін толық жауапты болады;
- 3) клиент атынан ForteX модулі арқылы жіберілген және Банк белгіленген қауіпсіздік процедураларына сәйкес орындауға қабылдаған құжаттардың санкцияланғаны үшін жауапкершілік пен міндеттемені өзіне алады.

(Ереже Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес 4-І Бөлімімен толықтырылды (отырыстың №53 хаттамасы)).

5. Электронды банктік қызметтерді көрсетуді тоқтата тұру/қайта жалғастыру және тоқтату

9. Электронды банктік қызметтерді көрсетуді тоқтата тұру тәртібі мен талаптары.

9.1. Банк келесі жағдайларда Клиентті алдын ала ескертусіз Электронды банктік қызметтерді көрсетуді тоқтатуға және/немесе Қолданушының/Клиенттің Уәкілетті өкілінің Электронды банктік қызметтерді алуға қолжетімділікті тоқтатуға құқылы:

- 9.1.1. Клиенттің Уәкілетті өкілі/Қолданушы Банк Клиенттен тиісті ауызша немесе жазбаша өтініш алған кезде жүйеге кіру үшін Клиенттің логинін және/немесе Қолданушының логинін және/немесе жылдам кіру ПИНін және/немесе ПИНді және/немесе Құрылған кодты және/немесе Digipass құрылғысын жоғалту/жариялау/үшінші тұлғаларға беру;
 - 9.1.2. Клиенттің Банктік шоттарына рұқсат қолжетімділіктің немесе Жүйені рұқсатсыз пайдалану орын алғандығына күдіктену;
 - 9.1.3. Клиенттің Электронды банктік қызмет көрсетілген Банктік шоты бойынша тыйым салынған және/немесе шығыс операциялардың тоқтатылуы және/немесе үшінші тұлғалар тарапынан орындалмаған талаптардың болуы.
 - 9.1.4. Шартта және/немесе Қазақстан Республикасының заңнамаларында қарастырылған басқа жағдайларда.
- 9.2. Клиенттің логинін және/немесе Қолданушының логинін және/немесе жылдам кіру ПИНін және/немесе ПИНді және/немесе Құрылған кодты және/немесе Digipass құрылғысын жоғалту/жариялау/үшінші тұлғаларға беру жағдайларында Электронды банктік қызметтерді көрсетуді тоқтатау және/немесе Қолданушының/Клиенттің Уәкілетті өкілінің Электронды банктік қызметтерге қолжетімділікті тоқтатуды Банк Клиенттің Шартта бұл көрсетілген болса Байланыс деректері бойынша Банкке Қолданушының/Клиенттің Уәкілетті өкілінің Банкке кодтық сөзді ауызша айтуы негізінде жүргізе алады.
- 9.3. Digipass құрылғысы Клиенттің кінәсінен бұзылған кезде, Digipass құрылғысының сыртқы зақымдануы кезінде (құрылғының экраны сынған және/немесе механикалық зақым келтірілген болса) және/немесе Digipass құрылғысы Клиенттің / Клиенттің уәкілетті өкілінің ПИНді дұрыс енгізбеуі салдарынан 3 реттен көп блокталған кезде (Digipass құрылғысы " LOCK DISABLED" хабарламасын көрсетеді), Клиенттің/оның уәкілетті өкілінің жазбаша өтініші негізінде Клиенттің/оның уәкілетті өкілінің Банкке жазбаша өтініші келіп түскен күннен бастап 3 (үш) жұмыс күнінен аспайтын мерзімде Digipass құрылғысын Банктің тарифтеріне сәйкес ақылы негізде ауыстыруды жүзеге асыру. Бұл ретте Digipass құрылғысын Клиент/оның уәкілетті өкілі Банктің қызметкеріне Digipass құрылғысының жұмыс істемейтін жай-күйінің себебін көрсете отырып, Digipass құрылғысының жұмыс істемейтін құрылғыны 2 данада қол қойылған қабылдау-тапсыру актісі, Digipass құрылғысының анықталған зақымдануларының "LOCK DISABLED" хабарламасы бар сипаттамасы/Банктің жауапты қызметкері және Клиент/оның уәкілетті өкіліне беріледі.
- 9.4. Digipass құрылғысының Клиентке/оның Уәкілетті өкіліне берілген Digipass құрылғысын берген сәттен бастап 3 (үш) айдан көп емес кезеңде анықталған/белгіленген жұмысқа жарамсыздық күйінде, айтарлықтай сыртқы ақаулары/«LOCK DISABLED» хабарламасы болмаған жағдайда, Клиенттің/оның Уәкілетті өкілінің жазбаша өтінішінің негізінде Digipass құрылғысын ауыстыруды электронды банктік қызметтерді көрсету ережелерінде белгіленген тәртіппен Клиенттің/оның уәкілетті тұлғасының Банкке жазбаша өтініші келіп түскен күннен бастап 3 (үш) жұмыс күнінен аспайтын мерзімде Банк тарифтеріне сәйкес төлем алмай-ақ жүзеге асыру. Осы тармақтың бірінші абзацында белгіленген мерзімнен кейін кез келген негіздер бойынша Digipass құрылғысының жұмысқа қабілеттілігін анықтау/анықтау кезінде Digipass құрылғысын ауыстыру осы Ереженің 10.3-тармағында көзделген тәртіппен Банк тарифтеріне сәйкес ақылы негізде жүзеге асырылады.
- 9.5. Уәкілетті орган тыйым салған және/немесе шығыс операцияларын тоқтата тұрған және/немесе клиенттің Электрондық банк қызметі көрсетілетін Банктік шоты бойынша үшінші тұлғалардың

орындалмаған талаптары болған жағдайда, Банк Электрондық банк қызметін көрсетуді тыйым салуды алып тастаған және/немесе шығыс операцияларын қайта бастаған және/немесе Клиенттің электрондық банк қызметі ұсынылатын банктік шотында үшінші тұлғалардың орындалмаған барлық талаптары орындалған кезге дейін тоқтата тұрады.

- 9.6. Клиенттің тиісті түрде ресімделген тиісті хатының негізінде Клиентке Электронды банктік қызметтерін көрсетуді тоқтата тұрған кезде және/немесе егер Клиенттің банк операцияларын жүргізу үшін көрсетілетін қызметтерге ақы төлеу бойынша банк алдында 30 (отыз) күнтізбелік күннен астам берешегі болса, Электронды банктік қызметтеріне қол жеткізу Клиенттің барлық Қолданушылары/Уәкілетті өкілдері үшін тоқтатыла тұрады. Клиенттің нақты Қолданушысы/Уәкілетті өкілі үшін Электронды банктік қызметтерге қол жеткізуді тоқтата тұру Клиенттің өзге Қолданушылары/Уәкілетті өкілдері үшін Электронды банктік қызметтерге қол жеткізуді тоқтата тұрмайды.

(Ереженің 5 бөліміне Басқарманың 2019 жылғы 16 мамырдағы шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы)).

(Ереженің 5 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

10. Электронды банктік қызметтерді көрсетуді қайта жалғастыру тәртібі мен талаптары.

- 10.1. Клиент жүйеге кіру үшін Қолданушының логинін және/немесе ПИН/Құпиясөзін және/немесе ПИН және/ немесе Digipass құрылғысын жоғалтқан/жария еткен/үшінші тұлғаларға берген жағдайда Электронды банк қызметтерін ұсынуды жалғастыру Клиенттің тиісті түрде ресімделген хатының және/немесе өтінімнің (Шартқа №1 қосымша) негізінде Клиентке Қолданушының жаңа логинін және/немесе «Заңды тұлғаларға арналған Интернет-банкинг» жүйесіне кіру үшін (бастапқы) ПИН-ді ұсынғаннан кейін/ Қолданушының/Клиенттің уәкілетті өкілінің «ForteBusiness» жүйесіне (бастапқы) және/немесе Digipass құрылғылары бергеннен кейін іске асырылады. Бұл ретте Клиентке қызмет көрсетілетін филиал бөлімшесінің жауапты қызметкері Клиент Банкке жазбаша өтініш берген күннен бастап 3 (үш) жұмыс күнінен аспайтын мерзім ішінде Клиент/Клиенттің Уәкілетті өкілі және филиал бөлімшесінің жауапты қызметкері қол қойған қабылдау-тапсыру актісі бойынша Қолданушының Жаңа логинін және/немесе жүйеге(бастапқы) және/немесе ПИН (бастапқы) және/немесе Digipass құрылғысына кіру үшін Клиентке/Клиенттің Уәкілетті өкіліне Қолданушының Жаңа логинін және / немесе жүйеге кірудің ПИНін (бастапқы) және/немесе Digipass құрылғысын дайындайды және береді.

- 10.2. Digipass құрылғысы Клиенттің / Клиенттің уәкілетті өкілінің Digipass құрылғысын қосу үшін ПИНді дұрыс енгізбеуі салдарынан 5 (бес) реттен көп бұғатталған кезде Электронды банктік қызметтерді қайта жалғастыру Клиенттің тиісті түрде ресімдеген хатының негізінде жүргізіледі. Бұл ретте Банк өз бетінше жоғарыда аталған негізде бұғаттауды 3 (үш) рет қана алып тастай алады, керісінше болған жағдайда Digipass құрылғысы бұғатталады және осы Ереженің 10.3 тармағында қарастырылған тәртіпте ауыстырлуы тиіс.

- 10.3. Клиенттің Банктік шоттарына рұқсатсыз қолжетімділікке күдік туындаған жағдай себебінен тоқтатылған Электронды банктік қызметтерді қайта жалғастыру Клиенттің тиісті түрде ресімделген хатының және/немесе Өтінімнің (Шарттың №1 Қосымшасы) негізінде және Банк Қолданушының/Клиенттің Уәкілетті өкілінің Қолданушы логинін, «Заңды тұлғаларға арналған интернет-банкинг» Жүйесіне кіруге арналған ПИН-кодты ауыстырған соң/«ForteBusiness» Жүйесінде Қолданушының/Клиенттің Уәкілетті өкілінің өз бетінше Құпиясөзді қалпына келтірген соң жүргізіледі. Бұл ретте Клиентке қызмет көрсетілетін филиалдың жауапты қызметкері Клиенттің Банкке жазған жазбаша өтінімін жазған күннен бастап 3 (үш) жұмыс күнінен асырмай Клиентке Клиентке/Клиенттің уәкілетті өкіліне жаңадан Қолданушының логинін және/немесе жүйеге кіруге арналған ПИНді дайындайды және Шарттың №2 Қосымшасына сәйкес Клиент/Клиенттің Уәкілетті өкілі мен Филиал Бөлімшесінің жауапты қызметкері қол қойған Қабылдау-тапсыру актісі бойынша береді.

- 10.4. Уәкілетті органдар тыйым салуды белгілеген және/немесе шығыс операцияларын тоқтата тұрған және/немесе Электронды банктік қызмет көрсетілетін Клиенттің банктік шотында үшінші тұлғалардың орындалмаған талаптарының орын алған жағдайында Электронды банктік қызметтерді ұсынуды қайта бастау тыйым салуды алып тастағаннан және/немесе шығыс операцияларын қайта бастағаннан және/немесе Электронды банктік қызмет ұсынылатын Клиенттің банктік шотында үшінші тұлғалардың орындалмаған барлық талаптары орындалғаннан кейін ғана жүргізіледі.

(Ереженің 5 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

11. Электронды банктік қызметтерді көрсетуді тоқтатудың тәртібі мен талаптары.

- 11.1. Банк келесі жағдайларда Клиентті алдын ала ескертусіз Электронды банктік қызметтерді көрсетуді тоқтатып тастауға құқылы:
- 11.1.1. егер Клиенттің Банк алдында банк операцияларын жүргізу бойынша қызметтерге төлем жасау бойынша 30 (отыз) күнтізбелік күннен астам берешегі болса;
 - 11.1.2. егер Клиенттің Банктегі барлық Банктік шоттары жабылған болса;
 - 11.1.3. Шартта және/немесе Қазақстан Республикасының заңнамаларында қарастырылған басқа жағдайларда.
- 11.2. Банк Шарт мерзімі аяқталған/бұзылған жағдайда Электронды банктік қызметтерді көрсетуді тоқтатуға құқылы. Электронды банктік қызметтерді көрсетуді тоқтатуға байланысты Шартты бұзу/әрекетін тоқтату тәртібі Шарттың талаптарына және/немесе Қазақстан Республикасының заңнамаларына сәйкес іске асырылады.

6. «Заңды тұлғаларға арналған интернет-банкинг» жүйесіндегі қауіпсіздік процедуралары

12. «Заңды тұлғаларға арналған интернет-банкинг» жүйесінде берілетін және алынатын ақпараттың құпиялылығын сақтауды қамтамасыз ету мақсатында TLS (Transport Layer Security — тасымал деңгейінің қауіпсіздігі) шифрлеу қолданылады. Шифрлеу Клиенттің деректерін «Заңды тұлғаларға арналған интернет-банкинг» Жүйесінде оларды интернет желісі арқылы жібермес бұрын шифрланған кодқа түрлендіреді және Банктің компьютерлік жүйесі мен Клиенттің Интернет-браузері арасындағы жолда Клиенттің ақпаратының құпиялылығын қамтамасыз етеді.
13. Клиент 256 bit шифрлеуді қолдау мүмкіндігін анықтау үшін браузерді тексеруді жүргізуге міндетті.
14. TLS – хаттама Клиентке Электронды банктік қызметтер ұсынылатын электронды құжаттардың мазмұнында бұрмаланулардың және / немесе өзгерістердің болуын анықтауға мүмкіндік береді.
15. «Заңды тұлғаларға арналған интернет-банкинг» Жүйесінде ықтимал қауіпті ақпараттың компьютерлік жүйелерге кіруін бұғаттау және «Заңды тұлғаларға арналған интернет-банкинг» Жүйесіне рұқсатсыз кірудің алдын алу үшін желіаралық экрандар (firewall/Brandmauer) пайдаланылады. Желіаралық экрандар бағдарламалық қамсыздандыру кеңселік және үйдегі компьютерлерге рұқсатсыз қолжетімдік пен вирустардан қорғау мақсатында орнатылады.
16. Банк Клиенттің компьютерін және Клиенттің «Заңды тұлғаларға арналған интернет-банкинг» Жүйесіне қосылған шоттары туралы ақпаратты қорғау мақсатында Банкпен байланыстың орнатылғандығын тексеру үшін цифрлы сертификаттарды қолданады. Клиент Сәйкестендірілген соң және «Заңды тұлғаларға арналған интернет-банкинг» Жүйесінде Аутентификацияланған кезде Банктің веб-сайтында Клиенттің браузері цифрлы сертификаттар арқылы Банктің веб-сайтын өзінің сәйкестендіру ақпаратымен растауды сұратады. Клиенттің браузері сертификатты тексере алады және егер веб-сайт Банкке тиесілі болмаса Клиентке ескерте алады. Сәйкестендіру кезінде Клиент бұл тексерудің қажеттілігіне көз жеткізе алады.
17. Қашықтан банктік қызмет көрсету сеансының қауіпсіздігі Қауіпсіз қосылулар хаттамасы (TLS) шифрлауы арқылы «қорғалған» ортада қамтамасыз етіледі. TLS технологиясы құпиялылықты сақтау мақсатында Клиенттің дербес ақпаратын шифрлау үшін қашықтан банктік қызмет көрсету сеансы аясында пайдаланылады.
18. Төлем қызметтерін көрсету кезінде Банк пен Клиент арасында ақпарат алмасу Digipass Құрылғысын, Клиентті қарқынды түрде сәйкестендіру деп аталатын Құрылған код арқылы іске асырылады.
19. Клиентті сәйкестендіру мақсатында «Заңды тұлғаларға арналған Интернет-банкинг» жүйесіне кіруді жүзеге асыру кезінде жүйеге кірген кезде мынадай сәйкестендіретін деректер көзделеді: Клиенттің логині, Қолданушының логині, Жүйеге кіруге арналған ПИН және Digipass құрылғысымен жасалған, осы Қолданушыға/Клиенттің Уәкілетті өкіліне тағайындалған/тиесілі Digipass құрылғысымен Құрылған код.
20. Клиенттен төлем қызметтерін алу кезінде Аутентификациялау мақсатында Digipass Құрылғысында жасалған Құрылған кодты міндетті енгізу қарастырылады.
21. Клиент үшінші тұлғаларға Клиенттің логинін, Қолданушының логинін, жүйеге кіруге арналған ПИНді, ПИНді, Құрылған кодты, Digipass құрылғысын жариялауға/беруге құқығы жоқ.
22. «Заңды тұлғаларға арналған интернет-банкинг» Жүйесінде қауіпсіздік мақсатында Клиенттің «Заңды тұлғаларға арналған интернет-банкинг» Жүйесіндегі ағымдағы сессияны өшіру қызметі қарастырылған. Клиенттің «Заңды тұлғаларға арналған интернет-банкинг» Жүйесіндегі ағымдағы сессиясын өшіру дегеніміз «Заңды тұлғаларға арналған интернет-банкинг» Жүйесінде Клиенттің ұзақ уақыт (10 минуттан көп) белсенді әрекет болмаған жағдайда (кез келген операцияларды іске асырмау, кез келген электронды құжаттарды ұсынбау және т.б.) Электронды банктік қызметтерді көрсетуді айтамыз.
23. Өтінімде көрсетілген деректерді растау мақсатында Банк телефон байланысы арқылы Клиенттің Өтінімде көрсетілген телефон нөмірі бойынша Клиенттің Өтінімін орындауға байланысты қажетті мәліметтерді алуға/нақтылауға құқылы.
24. Электронды банктік қызметтерді көрсету кезінде Банк қызметтерін ұсынуға негіз болған хабарламалардың жіберілгені және/немесе алынғаны туралы растайды. Егер Шартта басқасы

белгіленбеген болса, электронды хабарламаны алғандығын растау оны алғандығы туралы хатты алушыға жіберу арқылы жүргізіледі.

25. Клиенттің тиісті түрде ресімделген хатының негізінде Банк Клиенттің хатын алған күннен бастап 10 (он) жұмыс күнінің ішінде Клиенттің хатында көрсетілген жазбаша түрде (электронды пошта/«Заңды тұлғаларға арналған интернет-банкінг» Жүйесі/арнайы/курьерлік қызмет арқылы) Электронды банктік қызметтерді жібергендігі және/немесе алғандығы туралы растаманы жібереді. Шарттың қолданыс мерзімінің ішінде Банк ұсынатын электронды банктік қызметтердің шекті мерзімдері Қазақстан Республикасының заңнамаларында қарастырылған мерзімдерге сәйкес келеді.

(Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес 6 бөлімге өзгерістер енгізілді (отырыстың №53 хаттамасы)).

6-1. «Заңды тұлғаларға арналған «ForteBusiness» интернет-банкінгінде» және «ForteBusiness» Мобильді интернет-банкінгі» жүйелеріндегі қауіпсіздік процедуралары

Тарау Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес мобильді интернет-банкінг түсінігімен толықтырылған. 10.11.2021ж. №2021-489998 өтінім.

26. «ForteBusiness» Жүйесінде берілетін және алынатын ақпараттың құпиялылығын сақтауды қамтамасыз ету мақсатында TLS (Transport Layer Security — тасымал деңгейінің қауіпсіздігі) шифрлеу қолданылады. Шифрлеу Клиенттің деректерін «ForteBusiness» Жүйесінде оларды интернет желісі арқылы жібермес бұрын шифрланған кодқа түрлендіреді және Банктің компьютерлік жүйесі мен Клиенттің Интернет-браузері арасындағы жолда Клиенттің ақпаратының құпиялылығын қамтамасыз етеді.
27. Клиент 256 bit шифрлеуді қолдау мүмкіндігін анықтау үшін браузерді тексеруді жүргізуге міндетті.
28. TLS - хаттама Клиентке Электронды банктік қызметтер ұсынылатын электронды құжаттардың мазмұнында бұрмаланулардың және / немесе өзгерістердің болуын анықтауға мүмкіндік береді.
29. «ForteBusiness» Жүйесінде ықтимал қауіпті ақпараттың компьютерлік жүйелерге кіруін бұғаттау және ««ForteBusiness» Жүйесіне рұқсатсыз кірудің алдын алу үшін желіаралық экрандар (firewall/Brandmauer) пайдаланылады. Желіаралық экрандар бағдарламалық қамсыздандыру кеңселік және үйдегі компьютерлерге рұқсатсыз қолжетімдік пен вирустардан қорғау мақсатында орнатылады.
30. Банк Клиенттің компьютерін және Клиенттің «ForteBusiness» Жүйесіне қосылған шоттары туралы ақпаратты қорғау мақсатында Банспен байланыстың орнатылғандығын тексеру үшін цифрлы сертификаттарды қолданады. Клиент Сәйкестендірілген соң және «ForteBusiness» Жүйесінде Аутентификацияланған кезде Банктің веб-сайтында Клиенттің браузері цифрлы сертификаттар арқылы Банктің веб-сайтын өзінің сәйкестендіру ақпаратымен растауды сұратады. Клиенттің браузері сертификатты тексере алады және егер веб-сайт Банкке тиесілі болмаса Клиентке ескерте алады. Сәйкестендіру кезінде Клиент бұл тексерудің қажеттілігіне көз жеткізе алады.
31. Қашықтан банктік қызмет көрсету сеансының қауіпсіздігі Қауіпсіз қосылулар хаттамасы (TLS) шифрлеуі арқылы «қорғалған» ортада қамтамасыз етіледі. TLS технологиясы құпиялылықты сақтау мақсатында Клиенттің дербес ақпаратын шифрлеу үшін қашықтан банктік қызмет көрсету сеансы аясында пайдаланылады.
32. Төлем қызметтерін көрсету кезінде Банк пен Клиент арасында ақпарат алмасу Digipass Құрылғысын, Клиентті қарқынды түрде сәйкестендіру деп аталатын Құрылған код арқылы іске асырылады.
33. Клиентті сәйкестендіру мақсатында «ForteBusiness» жүйесіне кіруді жүзеге асыру кезінде жүйеге кірген кезде мынадай сәйкестендіретін деректер көзделеді: Клиенттің логині, Қолданушының логині, Жүйеге кіруге арналған ПИН және Digipass құрылғысымен жасалған, осы Қолданушыға/Клиенттің Уәкілетті өкіліне тағайындалған/тиесілі Digipass құрылғысымен Құрылған код.
34. Клиенттен төлем қызметтерін алу кезінде Аутентификациялау мақсатында Digipass Құрылғысында жасалған Құрылған кодты міндетті енгізу қарастырылады.
35. Клиент үшінші тұлғаларға Клиенттің логинін, Қолданушының логинін, жүйеге кіруге арналған ПИНді, ПИНді, Құрылған кодты, Digipass құрылғысын жариялауға/беруге құқығы жоқ.
36. «ForteBusiness» Жүйесінде қауіпсіздік мақсатында Клиенттің «Заңды тұлғаларға арналған интернет-банкінг» Жүйесіндегі ағымдағы сессияны өшіру қызметі қарастырылған. Клиенттің «ForteBusiness» Жүйесіндегі ағымдағы сессиясын өшіру дегеніміз «ForteBusiness» Жүйесінде Клиенттің ұзақ уақыт (10 минуттан көп) белсенді әрекет болмаған жағдайда (кез келген операцияларды іске асырмау, кез келген электронды құжаттарды ұсынбау және т.б.) Электронды банктік қызметтерді көрсетуді айтамыз.
37. Өтінімде көрсетілген деректерді растау мақсатында Банк телефон байланысы арқылы Клиенттің Өтінімде көрсетілген телефон нөмірі бойынша Клиенттің Өтінімін орындауға байланысты қажетті мәліметтерді алуға/нақтылауға құқылы.

38. Электронды банктік қызметтерді көрсету кезінде Банк қызметтерін ұсынуға негіз болған хабарламалардың жіберілгені және/немесе алынғаны туралы растайды. Егер Шартта басқасы белгіленбеген болса, электронды хабарламаны алғандығын растау оны алғандығы туралы хатты алушыға жіберу арқылы жүргізіледі.
39. Клиенттің тиісті түрде ресімделген хатының негізінде Банк Клиенттің хатын алған күннен бастап 10 (он) жұмыс күнінің ішінде Клиенттің хатында көрсетілген жазбаша түрде (электронды пошта«ForteBusiness» Жүйесі/арнайы/курьерлік қызмет арқылы) Электронды банктік қызметтерді жібергендігі және/немесе алғандығы туралы растаманы жібереді. Шарттың қолданыс мерзімінің ішінде Банк ұсынатын электронды банктік қызметтердің максималды мерзімдері Қазақстан Республикасының заңнамаларында қарастырылған мерзімдерге сәйкес келеді.
40. «ForteBusiness» Жүйесінде жұмыс істеу кезінде қауіпсіздікті қамтамсыз ету мақсатында Қолданушы келесі қағидаларды ұстануы тиіс:
- 1) мобильді қосымшаны және оның жаңартуларын Интернет желісіндегі мобильді операциялық жүйелерді өндірушілердің тек қана ресми онлайн дүкендерінен ғана орнату;
 - 2) лицензияланбаған, күмәнді, сонымен қатар зиянды бағдарламалардың бар екендігіне тексерілмеген бағдарламалық қамсыздандыруларды қолданбау;
 - 3) «ForteBusiness» Жүйесінде жұмыс істеу үшін шектеулі физикалық қолжетімділігі бар жеке компьютерді қолданған абзал;
 - 4) лицензияланған, уақтылы жаңартылатын бағдарламалық өамсыздандыруды пайдалану. Вирустардың әрекеті Қолданушының сәйкестендіру деректерін құртуға бағытталуы мүмкін;
 - 5) өз компьютеріңізде және мобильді құрылғыңызда, ондағы анықталған осалдықтарды жою мақсатында өндіруші компания ұсынған автоматты түрде уақтылы жаңартумен заманауи операциялық жүйелерді пайдалану. Операциялық жүйе мен компьютер шолғышының жаңартуларын үнемі орындаңыз, бұл қауіпсіздік деңгейін едәуір арттырады;
 - 6) компьютерге вирустарға тексерілмеген сыртқы ақпарат тасымалдағыштарды қоспаңыз;
 - 7) қосымша қауіпсіздікті қамтамсыз ету үшін кіру кезінде «виртуалды клавиатураны» қолдануға болады, бұл енгізілген символдарды қолды болу мүмкіндігін болдырмайды;
 - 8) жүйелік деңгейде модификациялау («рутирленген», rootkit) үрдісіне ұшыраған құрылғыны қолданбау;
 - 9) ешкімге құрылғының клавиатурасында теріліп жатқан құпиясөз цифрларының, Digipass Құрылғысында жасалған Құрылған кодтың, СМС-кодтың жиынтығын байқап қоюына жол бермеу;
 - 10) тіркелген нөмірі бар ұялы телефон жоғалған немесе ұрланған жағдайда - мобильді ұялы оператор арқылы тіркелген телефон нөмірін бұғаттау және Банкке «ForteBusiness» Жүйесіне қолжетімділікті бұғаттау қажеттігі туралы хабарлау;
 - 11) жұмысты аяқтаған соң «ForteBusiness» Жүйесінің терезесін «Шығу» батырмасын басу арқылы жабу және «ForteBusiness» Жүйесіндегі ағымдағы сессиясымен компьютерде немесе ұялы құрылғыда қараусыз қалдырмау;
 - 12) интернет-қосылуды орнататын бағдарламаларда, компьютердегі мәтіндік файлдарда немесе басқа да электрондық ақпарат тасығыштарда құпиясөздерді сақтамаңыз, себебі бұл ретте оны ұрлау және жария ету тәуекелі бар;
41. Банк мыналарға жауапкершілік алмайды:
- 1) банктік құпияны құрайтын ақпаратқа қолжетімділіктің келесі әрекеттер салдарынан орын алуы:
 - Қолданушының «ForteBusiness» Жүйесіне кіру үшін және операциялар жасау үшін қажетті Логинді, «ForteBusiness» Жүйесіне кіруге арналған ПИНді және Digipass Құрылғысында жасалған Құрылған кодты, СМС-кодты жария етуі;
 - Қолданушының «ForteBusiness» Жүйесіне қолжетімділікті қамтамсыз ететін ұялы телефонды немесе басқа құрылғыны үшінші тұлғаға беруі немесе жоғалтуы;
 - 2) шоттарда орналастырылған ақшаға рұқсатсыз қолжетімділіктің және операциялардың орындалуының келесі әрекеттер салдарынан орын алуы:
 - Қолданушының «ForteBusiness» Жүйесіне кіру үшін және операциялар жасау үшін қажетті Логинді, «ForteBusiness» Жүйесіне кіруге арналған ПИНді және Digipass Құрылғысында жасалған Құрылған кодты, СМС-кодты жария етуі;
 - Қолданушының «ForteBusiness» Жүйесіне қолжетімділікті қамтамсыз ететін ұялы телефонды немесе басқа құрылғыны үшінші тұлғаға беруі немесе жоғалтуы;
 - «ForteBusiness» Жүйесіне қолжетімділікті бұғаттау үшін Қолданушының Банкке уақтылы хабарласпауы;
 - Қолданушының осы айтылған әрекеттерді сақтамауы салдарынан Логиннің, «ForteBusiness» Жүйесіне кіруге арналған ПИН және Digipass Құрылғысында жасалған Құрылған кодтың, СМС-кодтың қолды болуы;
 - Қолданушының құжаттарды ресімдеу және шот/телефон нөмірлерін және деректемелерді көрсету кезінде жіберген қателіктері;

- байланыс арналарының қолды болуы салдарынан Қолданушы енгізген деректер мен жүргізілген операциялар жайлы ақпараттың бөгде тұлғалардың алуы;

- Қолданушының «ForteBusiness» Жүйесімен ашық жұмыс сессиясын қараусыз қалдыруы.

42-1. Клиенттің деректерінің сақталуын, Сәйкестендіру мен Аутентификациялауды бақылау үшін клиенттер ҚР ҰКО-дан алған ЭЦҚ кілттері қолданылады. ЭЦҚ кілттері мен сертификаттарын беру тәртібі ҚР ҰКО талаптарымен реттелген. ЭЦҚ-мен жұмыс істеу үшін Мобильді интернет-банкінг мына кітапханаларды қолданады:

- 1) ҚР ҰКО құрастырушысының жиынтығы (NCALayer, Kalkan Crypt) - Хэш қалыптастыру, «Fortebusiness» Жүйесінің ішкі жүйесінде ЭЦҚ құру, сонымен қоса ҚКО серверінде ЭЦҚ тексеру үшін;
- 2) ТУМАР-CSP - Хэш қалыптастыру, «Fortebusiness» Жүйесінің ішкі жүйесінде ЭЦҚ құру, сонымен қоса ҚКО серверінде ЭЦҚ тексеру үшін.

*Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес
10.11.2021ж. №2021-489998 өтінім.*

42-1 тармақпен толықтырылған.

42-2. Мобильді интернет-банкінгті пайдалану кезінде Сәйкестендіру мен Аутентификациялау мақсатында келесі сәйкестендіру деректері қарастырылады: Клиентке тиесілі жеке сәйкестендіру нөмірі, ұялы телефон нөмірі (логин), Құпиясөз, СМС-код, ЭЦҚ, биометрикалық мәліметтер, FaceID, TouchID, жылдам кіру ПИН-коды. Қауіпсіздік процедураларын сақтау мақсатында Клиент Құпиясөзді 60 (алпыс) күнтізбелік күн сайын 1 (бір) рет ауыстырып отыруы қажет.

*Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес
10.11.2021ж. №2021-489998 өтінім.*

42-2 тармақпен толықтырылған.

42-3. Мобильді интернет-банкінгте қауіпсіздікті қамтамасыз ету мақсатында Клиенттің ағымдағы сессиясын автоматты түрде өшіру қызметі қарастырылған. Мобильді интернет-банкінгте Клиенттің ағымдағы сессиясын автоматты түрде өшіру дегеніміз Клиенттің Мобильді интернет-банкінгте ұзақ уақыт (3 минуттан көп) белсенді әрекет болмаған жағдайда (кез келген операцияларды іске асырмау, кез келген электронды құжаттарды ұсынбау және т.б.) электронды банктік қызметтерді көрсетуді айтамыз. Банк Клиент жүргізген операциялардың дұрыстығын, растығын, шынайылығын тексеру үшін және рұқсат етілмеген сатып алулардың, алаяқтық әрекеттердің алдын алу, құпия ақпаратты жария етуді болдырмау немесе басқа да құқықбұзушылық әрекеттердің алдын алу мақсатында қосымша шарттар, талаптар қарастырылуы мүмкін.

*Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес
10.11.2021ж. №2021-489998 өтінім.*

42-3 тармақпен толықтырылған.

42-4. AppStore, PlayMarket сервистерінен мобильді қосымшаны (Мобильді интернет-банкінг) жүктеп алудан бұрын Клиентке Құпиялылық саясатының (осы Ереженің №2 Қосымшасы) қағидаларымен танысу ұсынылады.

*Басқарма Төрағасының м.а. Ш.М. Нұрымбеттің шешіміне сәйкес
10.11.2021ж. №2021-489998 өтінім.*

42-4 тармақпен толықтырылған.

(Ереженің 6 бөлімінеБасқарманың 2019 жылғы 16 мамырдағы шешіміне сәйкес толықтырулар енгізілген (отырыстың №16 хаттамасы).

(Ереженің 6 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

7. Қорытынды ережелер

42. Электронды банктік қызметтерді көрсетуге байланысты сұрақтар бойынша Клиент келесі Байланыс деректері бойынша хабарласа алады:

+7 (727) 258-40-40

+7 (727) 258-75-75

+7 (7172) 58-75-75

Ұялы телефоннан 7575

Факс: +7 (727) 259-67-87

E-mail: info@forte.bank

Банктің мекенжайы: Нұр-Сұлтан қ., Достық к-сі, 8/1

(Басқарманың 2017жылғы 05 шілдедегі шешіміне сәйкес 27тармаққа өзгерістер енгізілді (отырыстың №53 хаттамасы)).

43. Банк біржақты тәртіпте Байланыс деректеріне Клиентті осындай өзгертулер жайлы Банктің веб-сайтында (www.forte.kz) хабарлау арқылы өзгертулер енгізуге құқылы.
44. Банк біржақты тәртіпте Электронды банктік қызметтерді көрсету Ережесіне өзгерістер енгізуге және Клиент үшін қолжетімді Банк ресурсында жариялауға құқылы.
45. Осы Ережеде реттелмейтін басқа да мәселелер Қазақстан Республикасы заңнамасының нормаларына, Банктің ішкі құжаттарына, Шартқа және банк саясатында қабылданған іскерлік айналымның әдет-ғұрыптарына сәйкес реттеледі.

(Ереженің 6 бөліміне Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

«ForteBank» АҚ-та «Занды тұлғаларға арналған интернет-банкинг/«Fortebusiness» интернет-банкингі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкингі» жүйесін пайдалану арқылы заңды тұлғаларға/жеке кәсіпкерлерге электронды банктік қызмет көрсетудің ережелерінің

№1 ҚОСЫМШАСЫ

Digipass Құрылғысын пайдалану нұсқаулығы

«Занды тұлғаларға арналған интернет-банкинг/«Fortebusiness» жүйесін пайдаланатын клиенттер үшін ақпаратты қорғаудың жоғары деңгейін қамтамасыз ету үшін жүйеде VASCO Data Security компаниясы өндірген Digipass құрылғысы қолданылады. Бұл компания on-line режимде жұмыс істейтін жүйелерге арналған сәйкестендіру құрылғыларын өндірушілердің арасында әлемдік жетекші болып табылады. Digipass 270 құрылғысы жүйеге кіруге арналған, сонымен қатар құжаттарды тексеруге арналған бір реттік кодтарды құрады.

1) Digipass 270 құрылғысын қалай пайдалану керек?

1.1) Құрылғыны қалай қосады/өшіреді?

Digipass 270 құрылғысын қосу үшін  және  батырмаларын бірдей басу қажет. Құрылғыны өшіру үшін үшбұрышты  батырманы екі рет басу қажет. Құрылғы 30 секунд әрекетсіздік болған жағдайда автоматты түрде өшеді.

1.2) Бастапқы PIN-кодты қалай орнату керек?

Digipass 270 құрылғысын алғаш рет қолданған кезде қолданушы 5 сандық дербес PIN-кодты құрастырып, есте сақтау қажет.

Действие пользователя	Сообщение устройства Digipass
Включение устройства Digipass 270  и 	NEW PIN
Ввод персонального 5-значного PIN-кода	PIN CONF
Подтверждение нового PIN-кода (повторный ввод)	NEW PIN CONF APPLI _

1.3) PIN-кодты қалай өзгертуге болады?

Digipass 270 құрылғысын қолдану барысында ағымдағы PIN-кодты өзгертуге болады.

Действие пользователя	Сообщение устройства Digipass
Включение устройства Digipass 270  и 	PIN
Ввод текущего PIN-кода и удержание кнопки  в течение нескольких секунд	APPLI _ NEW PIN
Ввод нового PIN-кода	PIN CONF
Подтверждение нового PIN-кода (повторный ввод)	NEW PIN CONF

1.4) Бір реттік құпиясөзді қалай құруға болады?

Жүйеге кіру үшін Қолданушы тиісті өріске өзінің Қолданушы атын және Digipass 270 құрылғысы құрған сеанстық кодты енгізуі қажет.

Действие пользователя	Сообщение устройства Digipass
Включение устройства Digipass 270  и 	PIN
Ввод PIN-кода	APPLI
Нажатие кнопки 1	APPLI 1
Подтверждение нового PIN-кода (повторный ввод)	NEW PIN CONF

1.5) Құрылғының сыртқы қабын ашуға және басқа да әрекеттер жасауға қатаң түрде тыйым салынады!

2) Жіні қойылатын сұрақтар

2.1) PIN-код деген не?

PIN-код **4/5** цифрдан тұрады, оны тек осы құрылғының иесі Қолданушы ғана біледі. Егер PIN-кодді кездейсоқ жағдайда үшінші тұлға біліп қойса, оны дереу ауыстыру қажет. Қауіпсіздік мақсатында PIN-код өте қиын болуы шарт. Оны есте сақтау (жазып алудың қажеті жоқ) қажет және үшінші тұлғаларға жария етуге болмайды.

2.2) PIN-кодты қате терген жағдайда не істеу қажет?

PIN-кодты қате терген жағдайда экранда —FAIL X|| деген хабарлама шығады, бұл жерде X – қате енгізілген кодтың санын көрсететін 1 ден 5 дейінгі цифрлар. Мысалы, —FAIL 3|| деген хабарлама PIN-кодтың 3 рет қате енгізілгенін білдіреді. Егер PIN-код 5 рет қатарынан қате енгізілген болса, экран бетінде —LOCK PIN|| деген хабарлама шығады да, құрылғы бұғатталады. и устройство блокируется. Құрылғыны бұғаттан шығару үшін Банкке бару қажет.

2.3) Егер жүйе құрылғы жасаған сандарды қабылдамаса не істеу қажет?

Егер жүйе құрылғы жасаған сандарды қабылдамаса, онда құрылғы ұзақ уақыт әрекетсіз болғандықтан, PIN-кодты көп рет қате тергендіктен немесе басқа да себептерден банкте бұғатталған болуы мүмкін. Құрылғыны бұғаттан шығару үшін қызмет көрсететін Банк филиалына бару қажет.

2.4) Құрылғыны жоғалтқан жағдайда не істеу керек?

Құрылғыны жоғалтқан жағдайда бұл туралы дереу Банкке хабарлау қажет.

(Ереженің 1 Қосымшасына Басқарманың 09.07.2021 жылғы № 01/2021-78 шешіміне сәйкес толықтырулар енгізілген).

«ForteBank» АҚ-та «Занды тұлғаларға арналған интернет-банкинг/«Fortebusiness» интернет-банкингі және «Fortebusiness» заңды тұлғаларға арналған мобильді интернет-банкингі» жүйесін пайдалану арқылы заңды тұлғаларға/жеке кәсіпкерлерге электронды банктік қызмет көрсетудің ережелерінің

№2 ҚОСЫМШАСЫ

Құпиялылық саясаты

«ForteBank» АҚ (бұдан әрі мәтін бойынша — Банк) Сізге заңды тұлғаларға арналған «Fortebusiness» мобильді интернет-банкингіне (бұдан әрі мәтін бойынша – Жүйе) қызығушылық танытқаныңыз үшін алғыс білдіреді.

Клиенттің (бұдан әрі мәтін бойынша — Қолданушы) дербес деректерін қорғау Банк үшін маңызды болып табылады, сондықтан біз Жүйені пайдалану барысында жинақталып, өңделетін деректердің қорғалуына айрықша мән береміз.

Жүйе Қолданушыға өзара жасасқан банктік қызмет көрсету шартының(-тарының) аясында Банкпен қарым-қатынасты жүзеге асыруға мүмкіндік береді. Жүйені пайдалануға қолжетімділік алу Қолданушының осы Саясаттың талаптарымен сөзсіз келісетіндігін білдіреді.

Банк Жүйе Қолданушыдан алынған жеке мәліметтердің қауіпсіздігін қамтамасыз етеді. Осы Саясат Жүйе Қолданушыларынан сұратылатын деректердің тізімін, сонымен қатар осындай деректерді Банктің және басқа да тұлғалардың өңдеу тәсілдерін көрсету мақсатында жасалған. Осы Саясатта сондай-ақ Қолданушының дербес деректері сұратылуы немесе жария етілуі мүмкін болатын мақсаттар көрсетілген.

Қолданушымен жекелей жасалатын келісімдер арқылы Қолданушының дербес деректері сұратылатын немесе жария етілетін басқа да мақсаттар қарастырылуы мүмкін. Осы Саясатта сондай-ақ Қолданушы өздерінің дербес деректерінің құпия болып қалуы үшін қабылдауға тиіс негізгі сақтық шаралары көрсетілген.

1. Жүйені қолдану барысында Банк мыналарды жинауы, сұратуы және(немесе) пайдалануы/алуы мүмкін:
 - 1.1. Қолданушының орналасқан жері туралы ақпарат, геолокация, орналасқан жерінің нақты координаттары, Қолданушыға жақын Банк бөлімшелерін, банкоматтарды іздестіру үшін Қолданушының орналасқан жерінің шамамен алынған координаттары;
 - 1.2. фотоқұжаттар жасау, суретті және/немесе фотосуретті жасау және/немесе сақтау, медиа-материалдарды сақтау, Қолданушының мобильді құрылғысында суретті сақтау, Қолданушының фотосуретін Мобильді қосымшада көрсету, төлем үлгісін қосу және қажетті құжаттарды жүктеу үшін Қолданушының мобильді құрылғысының камерасына кіру, Қолданушының мобильді құрылғысының медиатекасына кіру (фотогалерея/бейне галерея);
 - 1.3. Қолданушы жайлы ақпарат: ЖСН/БСН, ұялы телефон нөмірі, сонымен қатар Қолданушының Жүйеге бастапқы және кейінгі сәйкестендірілуі үшін биометрикалық деректер (оның ішінде Face ID, Touch ID);
 - 1.4. электронды-цифрлы қолтаңба (ЭЦҚ) сертификаттарын жүктеу мақсатында Қолданушының мобильді құрылғысының файлдар мен деректерді сақтау орнына қолжетімділік;
 - 1.5. шығыс операцияларды растау үшін өңделген ОТР-кодты алу мақсатында Қолданушының мобильді құрылғысында орнатылған басқа да қосымшаларға қолжетімділік;
 - 1.6. Қолданушының мобильді құрылғысының жай-күйін, соның ішінде Қолданушының мобильді құрылғысының телефон нөмірін, Қолданушының мобильді құрылғысының ұялы байланыс желісі туралы ағымдағы ақпаратты, барлық ағымдағы қоңыраулардың күйін және мобильді қосымшада авторизация кезінде ұялы телефон нөмірін автоматты түрде толтыру үшін мобильді

- қосымшаны пайдалану қауіпсіздігін арттыру үшін Қолданушының мобильді құрылғысында тіркелген барлық тіркелу жазбаларының тізімін оқу үшін ғана қолжетімділік;
- 1.7. мобильді құрылғы жайлы ақпарат. Банк мобильді құрылғының моделі, операциялық жүйесінің нұсқасы, құрылғының бірегей сәйкестендіргіші сияқты Қолданушының мобильді құрылғы жайлы ақпаратты жинайды;
 - 1.8. сәйкестендіру үшін, сондай – ақ Қолданушының операцияларын растау үшін SMS-хабарлама түрінде Банк жіберген растау кодын автоматты түрде толтыру мақсатында Қолданушының мобильді құрылғысындағы SMS хабарламаларға қолжетімділік;
 - 1.9. жүргізілетін операциялар жайлы ақпарат. Тауарлар мен қызметтерге, ақша аударымдарына және басқаларына ақы төлеу операцияларын жүргізу кезінде Банк жасалған операциялардың орны, уақыты және сомасы туралы деректерді, ақы төлеу тәсілінің түрін, қызметтерді сатушы және (немесе) ұсынушы туралы деректерді, егер бар болса, операцияны жасау себебінің сипаттамасын, сондай-ақ жоғарыда көрсетілген операцияларды жасауға байланысты өзге де ақпаратты жинайды. Қолданушының мәліметтерін пайдалану барысында Банк осы Саясатты, оларды өндеу кезінде Банк клиенттерінің дербес деректерін қорғау туралы Ережені, сондай-ақ «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңын басшылыққа алады.
 2. Жүйе Қолданушының Банктің қызметтерін ұсыну және көрсету (Қолданушымен жасалған шартты орындау) үшін қажетті дербес деректерін жинайды және сақтайды.
 3. Қолданушының дербес деректеріне қатысты оның құпиялылығы сақталады, тек Қолданушының өзі жайлы осындай деректерді/ақпаратты шектеусіз тұлғалар тобына ортақ қолдану үшін өз еркімен беру жағдайларын қоспағанда.
 4. Банк Қолданушы жайлы ақпаратты Қазақстан Республикасының заңнамаларына сәйкес өзінің үлестес тұлғаларына, сондай-ақ жоғарыда көрсетілген мақсаттарда Банкпен байланысы бар серіктестерге және өзге компанияларға беруге құқылы. Бұл ретте Банктің үлестес тұлғалары, сондай-ақ серіктестері мен өзге компаниялар осы Саясатты ұстануға міндетті.
 5. Банк Қолданушының банктік құпия болып табылатын ақпаратына үшінші тұлғалардың рұқсатсыз қол жеткізуін болдырмау үшін қажетті шараларды іске асыруға міндеттенеді. Мұндай сипаттағы кез келген ақпарат үшінші тұлғаларға Қазақстан Республикасының заңнамасында, оның ішінде Қолданушы Банкке ұсынған келісімдерге сәйкес белгіленген тәртіппен ғана берілуі мүмкін.
 6. Құпиясөздерді, SMS-кодтарды пайдалану барысында Банктің қандай да бір құпия ақпаратты беруін немесе сақтауын көздеген жағдайларда, Банк үшінші тұлғалардың осындай ақпаратқа оны Қолданушыға бергенге дейін, сондай-ақ көрсетілген ақпаратты сақтау уақытында қолжетімділігін болдырмау үшін ұйымдастырушылық және техникалық сипаттағы барлық қажетті және Банкке қатысты болатын шараларды қабылдауға міндеттенеді.
 7. Қолданушы тіркелу жазбасының логині мен құпиясөзі секілді деректерін үшінші тұлғалардан құпия ұстауы тиіс. Қолданушы оның тіркелу жазбасын рұқсатсыз пайдаланылғандығына күдіктенген кез келген жағдайлар жайлы Банкке дереу хабарлауға міндеттенеді. Жүйені қауіпсіз пайдалану Қолданушының Банктің ұсыныстарын сақтауына да байланысты болады.