TTS шоғырландырылған қауіпсіздік рәсімдері

Клиент пен Банк арасында жасалған Шот жүргізу және Қызмет көрсету туралы жалпы шарттарға (немесе шоттарға қызмет көрсетудің өзге қолданылатын талаптарына) («Жалпы шарттар») сәйкес «Хабарламалар» Тарауында келтірілгендей, төменде келесі қызметтермен және желілік өзара әрекеттесу арналарымен байланысты Банктік өнімдерді дамыту департаменті (Citi Treasury және Trade Solutions) пайдаланатын қауіпсіздікті қамтамасыз ету рәсімдері («Рәсім») сипатталады.

- CitiDirect BE® (соның ішінде Банктік шоттарды электрондық басқару (“eBAM”), TreasuryVision® және WorldLink®)
- Интерактивті ауызша жауап (“IVR”)
- Қағаз тасымалдаушы нысанындағы төлем нұсқаулықтарын (MIFT) ескермегенде, Банкпен аралдағы электрондық пошта/факс
- CitiConnect®
- Өзге жергілікті электрондық байланыс арналары

Қызметтердің немесе байланыс арналарының қолжетімдігі жергілікті нарықтардың жағдайларына байланысты ауытқитын болады. Осы рәсімдер уақыт өте келе қайта өзгертілуі мүмкін және сондай өзгертулер Клиентке электрондық байланыс құралдарының көмегімен немесе өзге әдіспен ұсынылуы мүмкін. Егер Клиент рәсімдерді қайта қарастыру және жаңарту туралы ақпараттандырылғаннан кейін жоғарыда келтірілген Қызметтердің немесе байланыс арналарының кез-келгенін пайдалануды жалғастырса (оған сонымен қатар, қызметтерді немесе ақпаратты байланыс арналары арқылы қайта қарастырумен / жаңартумен байланысты CitiDirect BE-де жаңартылған деректерді жариялау кіреді), онда бұл Клиенттің қайта қарастырылған рәсімдерді қабылдауы деп есептеледі. Осы рәсімдер Жалпы шарттармен бірге зерделенуі тиіс, себебі уақыт өте келе Жалпы шарттарға өзгертулер енгізілуі мүмкін. Анықтамасы осы құжатта келтірілген, бас әріппен жазылған терминдердің оларға Жалпы шарттарда берілген мәндері болуы тиіс.

A. Әкімшінің атқарымдары мен міндеттері*

CitiDirect BE-де қолжетімді қосымшалар үшін нұсқаулықтары енгізу және авторизациялау үшін екі жеке адам қажет, сондықтан кем дегенде екі Әкімші талап етіледі. Кез-келген екі Әкімші бірге әрекет ете отырып, Әкімшінің кез-келген атқарымына қатысты немесе Ғаламтор арқылы біздің өзара әрекеттесуімізді жеңілдетуіне байланысты, байланыс арналары арқылы нұсқаулықтар және/немесе растамалар бере алады. Осындай байланыс арналары арқылы өтетін осындай кез-келген хабарламалар екі Әкімшімен авторизацияланған кезде Банкпен қабылданып, өңделетін болады. Тиісті резервтік көшіруді қамтамасыз ету үшін Банкке кем дегенде үш Әкімші тағайындауға кеңес беріледі. Клиент өзінің Әкімшілерін Арналарға Каналдарға қосуға өтінішті қолдана отырып, тағайындайды. Клиенттің Әкімшісі сонымен қатар

үшінші тұлға-компаниялардың (мысалы, Клиенттің аффилиирленген кәсіпорнының) Шот(-тар)ы үшін Әкімшісі ретінде әрекет ете алады және қандай да бір қосымша тағайындауларсыз, осымен байланысты барлық құқықтарды іске асыра алады (соның ішінде осындай үшінші тұлғаның-компанияның Шот(-тар)ы үшін пайдаланушыларды тағайындау), егер осындай үшінші тұлға-компания Жан-жақты қолжетімділікке рұқсат нысанына (немесе Банк үшін қолайлы болып табылатын кез-келген қолжетімділікті авторизациялау нысанына) қол қойып, Клиентке оның Шот(-тар)ына қолжетімдік берсе. Бұл тиісті рұқсат таралатын Шотқа (шоттарға) қатысты ғана қолданылады.

* Әкімшінің атқарымдары мен міндеттеріне белгілі жергілікті нарықта тыйым салынуы мүмкін. Қосымша ақпарат алу үшін Клиенттерге операциялық қызмет көрсету қызметінің өкілдерімен байланысыңыз.

Сонымен қатар, Әкімші атқарымына мыналар кіреді:

1. Пайдаланушылардың қолжетімдігі мен құқықтарын тағайыдау және ағымдағы қолдауы (соның ішінде Әкімшілердің өздері), соның ішінде мынадай қызмет:

    (a) Пайдаланушылардың бейіндерін (соның ішінде Әкімшілердің бейіндері) және пайдаланушылардың құқықтарын қалыптастыру, жою немесе өзгерту (пайдаланушының есімі сәйкестендіру құжаттарына сәйкес келуі тиіс екеніне назар аударыңыз);

    (b) әртүрлі пайдаланушыларға қолжетімді атқарымдар мен деректерді анықтайтын қолжетімдік бейіндерін жасау;

    (c) жүйеге кірудің есептік деректерін қосу және сөндіру.

2. Клиенттер қолдайтын деректеме қоймалар ақпараттық жүйелерде (мұрағаттарда) жазбаларды (белгіленген пішімдердегі төлемдер және бенефициарлардың кітапханалық жүйелері) қалыптастыру және өзгерту, сондай-ақ басқа пайдаланушыларды дәл осындай әрекеттерді орындау үшін рұқсаттар беру.

3. Төлемдерді авторизациялау (мақұлдау) тізбегін өзгерту.

4. Клиенттің пайдаланушылары үшін жүйеге қолжетімдік деректемелері динамикалық сәйкестендірушіні немесе жүйеге қолжетімдік құпия сөздерін беру.

5. Қауіпсіздіктің беделі бұзылғанына қатысты кез-келген күдік туындаған кезде Банкке хабарлау.

Әкімшілер Клиенттің қолжетімдігі бар Банк өнімдерін пайдаланушылар үшін операциялар лимиттерін тағайындайды (белгілейді). Банк осы лимиттерді бақыламайды / мақұлдамайды; Клиент Клиенттің ішкі саясаттары мен талаптарының, соның ішінде Клиенттің Директорлар кеңесі немесе оған тең дәрежедегі орган тағайындаған өзге лимиттердің орындалуын қамтамасыз ету мақсатында өзі мониторинг жүргізуі тиіс.

Атап айтсақ, **eBAM қосымшасы** үшін келесі тұлғаларды тағайындау қажет:

Атқарымдарды / деректерге қолжетімдікті орындаудың пайдаланушылық құқықтарын күйлеу және анықтау үшін, сондай-ақ үдерістің бірізді әрекеттерін анықтау үшін екі жекелеген Аға әкімші жасаушы / тексеруші ретінде келісіп әрекет етеді. Банк осындай күйлеулерді бақыламайды / тексермейді; Клиенттің (сондай-ақ Шот иесінің) ішкі саясаттарын ұстануды, сондай-ақ талаптарды авторизациялау және келісу деңгейлерін орындауды, сонымен қатар Клиенттің Директорлар кеңесі (Шоттардың иелері) немесе баламалы құзыретті орган тағайындаған талаптарды орындауын қамтамасыз ету мақсатында Клиент пайдаланушының әрекеттерінің бірізділігін және қызметін бақылайды.

eBAM қызметі үшін келесі тұлғаларды тағайындау талап етіледі:

1. **Қауіпсіздік қызметкері:** жоғарыдағы (1) a-c тармақтарыда көрсетілген атқарымдарды Әкімшінің атқарымдары аясында орындайды.

2. **Корпоративтік хатшы:** Авторизациялаудың реттілігі, Пайдаланушыларды Авторизациялаушылар ретінде тағайындау, және оларды Мақұлдау Реттелігі аясында тағайындау Клиенттің (сондай-ақ Шот иегерінің) ішкі саясаттарына, авторизациялау деңгейіне және мақұлдауына, соның ішінде өзгелерден басқа, Клиенттің Директорлар (Шот иегерінің) кеңесімен немесе тең дәрежелі құзыретті органмен белгілен талаптарға сәйкес келуін қамтамасыз етеді.

3. **Авторизациялаушы:** жұмыс үдерісі аясындағы қызметке әрекет ету үшін және авторизациялау үшін кең, аға өкілеттіктері бар.

4. **Сұраныстарды бастамалаушылар:** бұл өтінімдерді рәсімдеу және шот жасау жөніндегі өтінім және eBAM жүйесінде қол қоюшылардың тізбесін басқару сияқты әкімшілендіру жөніндегі әрекеттерді орындауға уәкілетті тұлғалар.

Қауіпсіздік қызметкерлері, Корпоративтік хатшы және Авторизациялаушылар мыналар үшін жауап береді:

a) Бағыныш сатыны тағайындауды анықтау және әкімшілендіру және сайтты / ағысты басқару, мысалы, авторизациялаудың реттілігін тағайындау, Пайдаланушыларды айқындау және мақұлдау деңгейлерін айқындау;

b) Аға әкімшілердің қосымша рөлдерін қалыптастыру және Пайдаланушыларды (Клиенттің жұмыскерлері болуы міндетті емес) тағайындау;

c) Егер пайдаланушының (соның ішінде Аға әкімшілердің) кез-келген құқықтарының қауіпсіздігі немесе құпиялылығы бұзылды немесе беделі түсірілді деп күдіктенуге негіздеме болса, онда Банктің хабарламасы;

d) Клиентке қызметтерді және/немесе өнімдерді ұсынумен байланысты Банк уақыт өте келе негізді түрде сұрата алатын, Клиент толтыратын нысандарды қажет болу шамасына қарай толтыру, өзгерістер енгізу, мақұлдау және/немесе толықтыру.

B. Түпнұсқаландыру әдістері

Рәсімдер белгілі бір қорғалған түпнұсқаландыруды («Түпнұқсаландыру әдістері») қамтиды, олар әдетте Клиент немесе пайдаланушы өзі тіркелген немесе сәйкестендірілетін әрбір кезде қызметтерге немесе байланыс арналарына қолжетімділікке ие болу үшін қолданылатын динамикалық құпиясөзді генерациялайтын пайдаланушының бірегей сәйкестендіруші жұбы/құпия сөз, санды сертификаттар және қауіпсіздік токені сияқты механизмдері арқылы Клиенттің және/немесе оның кез келген пайдаланушысының өкілеттіктерін дұрыс түпнұсқаландыру және тексеру үшін қолданылады. Төменде сипатталған Түпнұсқаландыру әдістерінің қолжетімдігі жергілікті нарықтар талаптарына байланысты екеніне назар аударған жөн.

Әкімшілер және (а) операцияларды бастамалағысы немесе мақұлдағысы келетін (және Пайдаланушы бейіні осыны жасауға мүмкіндік беретін) және/немесе (б) иеленушінің құқықтарына сәйкес жүйелерге қолжетімдік алғысы келетін барлық пайдаланушылар қолжетімді түпнұсқаландыру әдістерін (уақыт өте келе жоғарыда сипатталғандай жаңарта алатын) пайдалануы тиіс.

Келесі Түпнұсқаландыру әдістері жоғарыда аталған қызметтерге және байланыс арналарына пайдаланушыны сәйкестендіргішпен (User ID) үйлесе отырып пайдаланылады:

Түпнұсқаландыру әдістері	**Сипаттамасы**
Токен: шақырту-жауап механизмі	Не болмаса (i) ұялы бағдарламалық токен (Mobile Soft Token) (ұялы қосымшаның негізінде) (мысалы, MobilePASS), не болмаса (ii) әр жағдайда 4-белгілі пин-кодтың көмегімен түпнұсқаландырғаннан кейін динамикалық құпия сөзді генерациялау үшін пайдаланылатын шифрлеудің атқарымдарын аппараттық іске асыратын токен (мысалы, SafeWord Card, Vasco). CitiDirect BE-ге қолжетімдік кезінде жүйе шақыртуды генерациялайды, ал жауаптық құпия сөз-код қолданылатын токеннің көмегімен генерацияланады және жүйеге енгізіледі.
Токен: бір реттік құпия сөз	Не болмаса (i) ұялы бағдарламалық токен (Mobile Soft Token) (ұялы қосымшаның негізінде) (мысалы, MobilePASS), не болмаса (ii) әр жағдайда 4-белгілі пин-кодтың көмегімен түпнұсқаландырғаннан кейін динамикалық құпия сөзді генерациялау үшін пайдаланылатын шифрлеудің атқарымдарын аппараттық іске асыратын токен (мысалы, SafeWord Card, Vasco). Осы динамикалық құпия сөз қолжетімдік алу үшін жүйеге енгізіледі.
SMS бойынша бір реттік код	Динамикалық құпия сөз пайдаланушыға SMS арқылы жіберіледі, осыдан кейін жүйеге қолжетімдік алу үшін пайдаланушы динамикалық құпия сөзді және қорғалған құпия сөзді енгізеді.

Бір реттік дауыстық код	Динамикалық құпия сөз пайдаланушыға автоматты дауыстық шақыртудың көмегімен беріледі, осыдан кейін жүйеге қолжетімдік алу үшін пайдаланушы динамикалық құпия сөзді және қорғалған құпия сөзді енгізеді.
Көп факторлық түпнұсқаландыру	Динамикалық құпия сөз SafeWord Card немесе MobilePASS токенінің көмегімен генерацияланады, осыдан кейін жүйеге қолжетімдік алу үшін осындай динамикалық құпия сөз қорғалған құпия сөзбен бірге енгізіледі.
Сандық сертификаттар	Уәкілетті сертификаттау органы берген және түпнұсқаландыру үшін пайдаланылатын сандық сертификат. Сандық сертификаттар кілтті және тиісті PIN-кодты сақтау механизмін пайдаланады және оны IdenTrust, SWIFT (3SKey) немесе өзге келісілген провайдерлер шығара алады.
Қауіпсіз құпия сөз	Жүйеге қолжетімдік алу үшін пайдаланушы өзінің қауіпсіз құпия сөзін енгізеді. Қауіпсіз құпия сөз әдетте пайдаланушының жүйедегі мүмкіндіктерін шектейді, сондықтан ақпаратты қарап шығуға болады, бірақ операция жүргізуге мүмкіндік жоқ.
Интерактивті дауыстық жауап (“IVR”) және электрондық пошта	Банкке жүгінетін пайдаланушыларға PIN-кодты енгізу немесе авторластырылған қолжетімдікті растау үшін телефон немесе электрондық пошта арқылы өзге апаратты беру ұсынылады
Факс	Банк алған құжатта, MIFT өтінімдерінен басқа, Клиенттің Директорлар кеңесінің шешімінде келтірілген ақпараттың негізінде қолтаңбаның түпнұсқалылығы тексерілетін болады.
MTLS	Mandatory Transport Layer Security хаттамасы (MTLS) (Көліктік деңгейді қорғау хаттамасы) банк пен сыртқы тарап арасында электрондық пошта бойынша қауіпсіз жекеше қосылысты жасайды. Осы арнаны пайдалану арқылы қолданған электрондық хат біріктіру арқылы жасалған TLS шифрленген туннель арқылы Ғаламтор арқылы жолданады.
Құпия сөзбен қорғалған PDF файлы	Шифрленген электрондық хаттар кәдімгі пошталық жәшікке PDF пішіміндегі құжат түрінде жеткізіледі, ол жеке құпия сөздің көмегімен ашылады, бұл ретте хабарламаның өзі және бекітілген барлық файлдар шифрленген. Қорғалған электрондық пошта арқылы алғашқы хабарламаны алғаннан кейін жеке құпия сөзді күйлеуге болады.

Түпнұсқаландырудың осы әдістерінің кез-келгені туралы анағұрлым толық ақпарат CitiDirect BE®-гі Login Help парағында ұсынылған:

(https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

CitiConnect® үшін

- Егер Клиент Citi-ге қосылу үшін жалпы қолжетімді ғаламтор-қосылысын, соның ішінде HTTPS хаттамасын FTP және FTPS қорғалған хаттамаларын пайдалануды тілесе, онда байланыс арнасы да, жолданатын хабарламалар да толықтай шифрланғанына және қорғалғанына кепілдік беру үшін Банк пен Клиент қауіпсіздік сертификаттарымен алмасады. Банк алмасу нәтижесінде алынған қауіпсіздік сертификаттарын пайдалану арқылы Клиенттің қорғалған байланыс шлюзінен келген хабарламаларды ғана қабылдайды

және керісінше, Банк алған қауіпсіздік сертификатының көмегімен Клиенттің байланыс шлюзіне ғана хабарламаларды жолдайтын болады.

- Егер Клиент SWIFT арқылы CitiConnect пайдаланушы шешсе, онда SWIFT-пен байланысты кез-келген төлем тапсырмалары мен жарлықтар үшін, соның ішінде осындай төлем тапсырмаларын өзгерту немесе болдырмау үшін, төлем тапсырмасы немесе жарлық Клиенттең шыққан екенін және оны Клиент авторизациялағанын тексеру үшін SWIFT Шарттық құжаттамасында қарастырылған Рәсімдер қолданылуы тиіс (осы термин SWIFT шартында келтірілгендей, оған уақыт өте келе енгізілетін түзетулер мен толықтыруларды ескере отырып), оған сонымен қатар Жалпы шарттар және FIN қызметі немесе SWIFT тағайындауы мүмкін өзге кез-келген шарттарда көрсетілгендер кіруі мүмкін. Банк SWIFT жүйесіндегі қандай да бір қателер немесе кідірістер үшін жауапкершілік тартпайды. Банкке хабарламалар SWIFT талап ететін және көрсетілген пішімде және түрде жолдануы тиіс.

- VPN Клиент пайдаланған кезде Клиент пен Банк арасында хабарламалар жіберілетін және/немесе алынатын бір IP-мекен-жайды Клиент пен Банк көрсетеді. Банк Клиенттің IP-мекен-жайынан шығатын хабарламаларды ғана қабылдайтын болады және керісінше, Банкте Клиент көрсеткен IP-мекен-жайға хабарламаларды жолдайтын болады.

- Клиент пен Банк сондай-ақ VPN түпнұсқаландыруына қосымша ретінде деректерді қорғаудың аппараттық модулін Түпнұсқаландыру әдістерін пайдалана алады. Бұл үшін Банк пен Клиент арасында хабарламаларды тарату үшін арналған серверлердегі құрылғыны Банк пен Клиенттің орнатуы қажет.

Банк талап етеді:

- Клиенттің Түпнұсқаландыру әдістерін қолдануына қатысты қауіпсіздік шараларын қабылдауы, атап айтсақ, соның ішінде жүйеге қолжетімдік параметрлерін (логин, құпия сөз) тексеру және/немесе Түпнұсқаландыру әдістерімен байланысты қауіпсіздік сертификаттары (бірлесіп «Жүйеге кіру үшін авторластыру деректері» деп аталады) және жүйеге кіру үшін қолжетімдік пен авторизациялау деректері Клиент уәкілеттеген тұлғаларда ғана болуын қамтамасыз етуы. Түпнұсқаландыру әдістері және жүйеге кіру үшін олармен байланысты авторизациялау деректері - осылардың көмегімен Клиент Банкке жолдаған хабарламаларды Банк тексеретін әдістер.

- Жүйеге кіру үшін Клиент деректерді қорғау үшін барлық саналы шараларды қабылдауы тиіс. Сәйкесінше, Банк Клиентке Авторизациялау деректерін үшінші тұлғалардың жүйеге кіруі үшін табыстамауға кеңес береді.

Кейбір құзыреттерде белгілі атқарымдарды орындауға қолжетімдік берілмес бұрын тұлғалар (және жүйеге кіру үшін олардың тиісті авторизациялау деректері) қылмыстық жолмен алынған ақшаны заңдастыруға қарсы әрекет ету туралы заңнаманың қолданыстағы талаптарына сәйкестікке қатысты сәйкестендірілуі тиіс.

Клиент кейбір жағдайларда Клиенттің авторизациялау деректерін жүйеге Клиенттің авторизациялау деректеріне қолжетімдікті ұсыну үшін Клиент көрсеткен бөгде тұлғалар немесе

қызметтердің провайдерлері (оның ішінде, сонымен қатар, үшінші тұлға болып табылатын еңбекақыны есептеу жөніндегі қызметтерді жеткізуші) (осындай үшінші тұлғалар немесе қызметтердің провайдерлері бұдан әрі «Уәкілетті үшінші тұлғалар» деп аталады) кез-келген банктік электрондық арналарға Клиенттің атынан қолжетімдік алу немесе пайдалану мақсатында кіру үшін табыстауды қалауға құқылы кейбір жағдайлар болатынын түсінеді. Клиент өзінің авторизациялау деректерін жүйеге Уәкілетті үшінші тұлғалардың кіруі үшін ұсынуды шешкен жағдайда, кез-келген Уәкілетті үшінші тарап Авторизациялау деректері үшінші тараптың авторизацияланбаған қызметкерлеріне ашылудан қорғау үшін барлық қолайлы шараларды Клиент өзі қабылдауына және қамтамасыз етуіне Банк кеңес береді. Уәкілетті үшінші тараптан осы Рәсімге сәйкес Клиенттің атынан хабарламаны алғаннан кейін Банк әрекет етуге уәкілеттенеді.

C. Деректердің бүтіндігі және Қорғалған байланыс

- Клиент Ғаламторды, электрондық поштаны және/немесе факсты пайдалана отырып, деректерді табыстай алады және Банкпен өзгеше әдіспен хабарламаларды алмасатын болады, және осы құралдар байланыстың және деректерді таратудың қауіпсіз жүйелері болуы міндетті емес. Банк салада қолданылатын озық шифрлеу әдістерін (Банкпен қолайлы деп анықтаған) пайдаланады, олар ақпараттың құпиялылығын және тарату кезінде деректердің өзгертілуін мүмкін болмауын қамтамасыз етуге көмектеседі.

- Егер Клиент Банктің қызметтерін, қосу арналарын немесе түпнұсқаландыру әдістерін кез-келген тұлға (ол уәкілетті тұлға екеніне немесе уәкілетті тұлға еместігіне қарамастан) тиісті түрде пайдаланбағаны немесе рұқсат етілмеген қолжетімдігі немесе техникалық кідірісі туралы күдіктенсе немесе оған мәлім болса, онда Клиент бұл туралы Банкке дереу хабарлауы тиіс. Егер, Клиенттің уәкілетті тұлғасы қызметтерге немесе арналарға қолжетімдікті немесе пайдалануды тиісті емес түрде іске қолданған жағдайда осындай тұлғаның Банктің қызметтеріне және байланыс арналарына қолжетімдігін және пайдалануын тоқтату үшін Клиент дереу тиісті шараларды қабылдауы тиіс.

- Егер Клиенттің деректері мен нұсқаулықтарын форматтау және айырып тануды қолдау үшін Клиент файлдарды форматтауға және шифрлеуге арналған бағдарламалық қамтамасыздандыруды (оны Банк немесе үшінші тұлға ұсынғанына қарамастан) пайдаланса және Citi-мен арадағы хабарламаларға қатысты әрекет етсе, онда Клиент осындай бағдарламалық қамтамасыздандыруды ол белгіленген мақсаттары үшін ғана пайдаланатын болады.

- (i) Авторластыру деректерін рұқсат етілмеген пайдалануға немесе алаяқтыққа қатысты күдік туындаған жағдайда және/немесе (ii) Қызметтерді және/немесе авторизациялау деректерін қорғау үшін жүйеге қолжетімдік алу үшін Авторизациялау деректерін пайдалануды талап ететін Қызметтерге Пайдаланушылардың қолжетімдігін Банк уақытша тоқтата алады дегенмен Клиент келіседі.